Google Ads

AdSpam Strategy Summit

June 23-24, 2020

Host: subir

Amit

GOOG-DOJ-AT-00554706

GOOG-DOJ-AT-00554707

DTX-951 Page 4 of 181

GOOG-DOJ-AT-00554708

Logistics Reminder

- Please stick to allocated time. Reminders issued when 5 mins left

- Follow presenter's guidance: asking questions during or after the presentation

- Any required follow ups/additional questions past time – enter them directly to the notes doc

- Note takers – keep AIs and follow up discussion in go/adspam-strategysummit20-notes

Google

Misha - 40 sec

GOOG-DOJ-AT-00554709

GOOG-DOJ-AT-00554710

DTX-951 Page 7 of 181

Speaker: Subir

GOOG-DOJ-AT-00554711
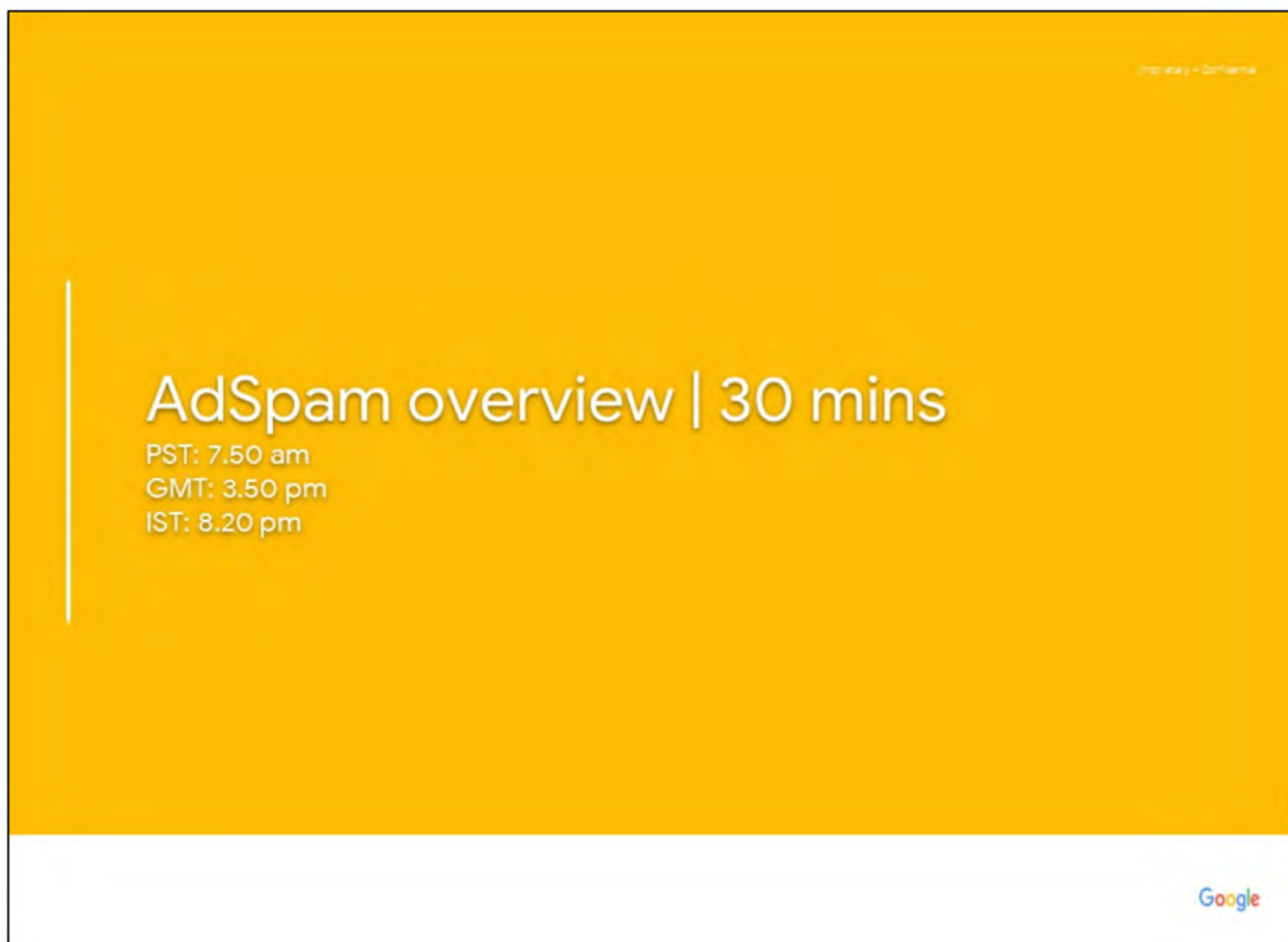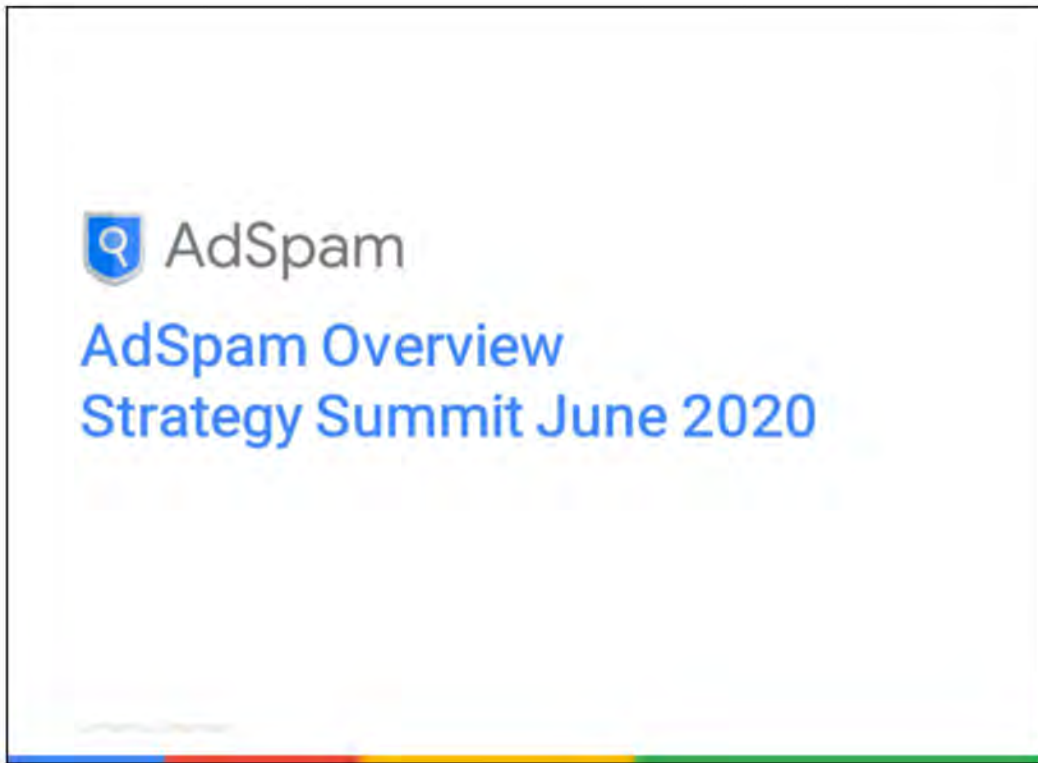
Mission can help answer the big questions...

Strategy summit goal

Set the foundation for our 2021+ planning.

Understand and align around key challenges
we need to address over the next few years.

Google

Alignment on and understanding of key challenges to prepare for 2021 planning (prepare for writing strategy docs for the APaS summit.

GOOG-DOJ-AT-00554713

AdSpam's mission

Defend against invalid traffic to build trust in the digital ads ecosystem and support healthy growth of Google's ads business

Google
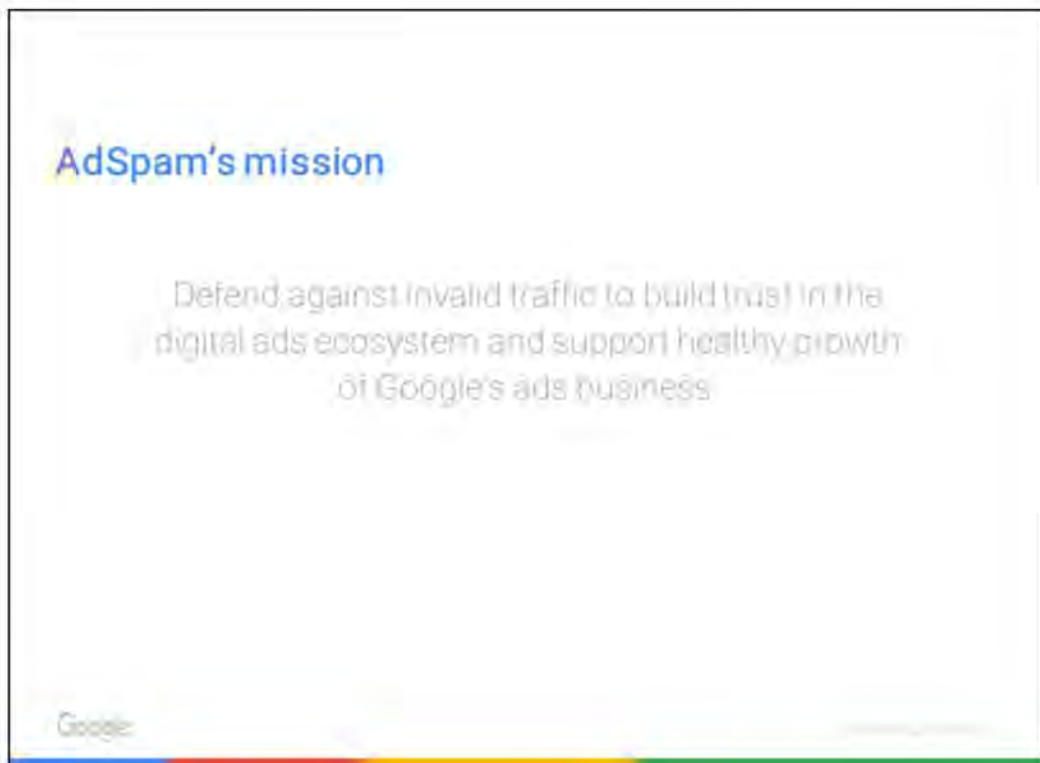
The words may be different between how T&S states the mission and how eng states it, but they are both are closely aligned on defending our ads ecosystem against IVT. Puneet explain that T&S' mission closely aligned.

GOOG-DOJ-AT-00554714
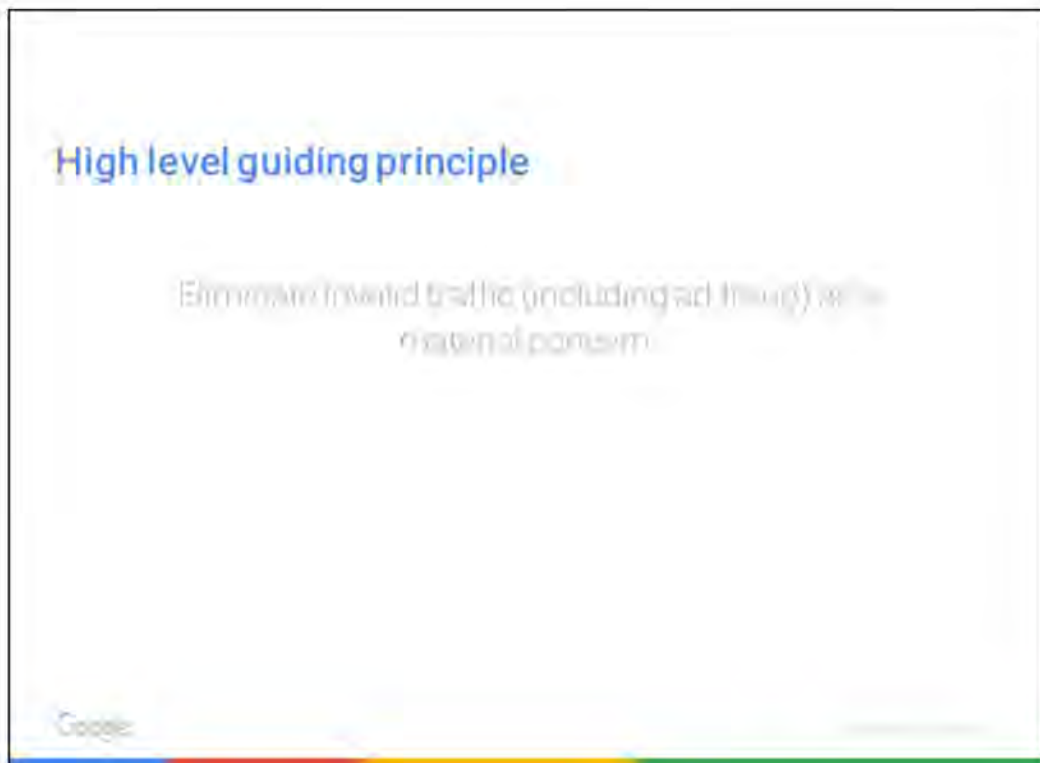
Speaker: Per
Invalid traffic should not be material enough to impact or affect where or how an advertiser allocates budget.

Online advertising ought to get to the same point as some other "mature" areas - for example credit card: As long as you take basic precautions, few credit card holders have material concerns about credit card fraud. Our dream is a future world where advertisers that take basic precautions (e.g., not buy "too cheap to be true" inventory from questionable sources that are not accredited) will not have to worry about invalid traffic and ad fraud in any material way.

Note: As with most other security/fraud areas, we'll "never be completely done". After achieving the "end state" we expect to continue to invest in invalid traffic defenses to maintain that "end state".
Overall guiding principles are available in docs (provide references[1][2])

GOOG-DOJ-AT-00554715

Strategic intent (long-term)

Defended and undefended IVT < 1% with less than $10M confirmed leakage/overfiltration due to client escalations for 1 year

See go/strategic-intent *for an explanation of strategic intent*

Google

Speaker: Per
This is a bit of a moonshot. Reminder that SI needs to be specific - know when you reach it.
Note that this includes defended (aka caught), undefended (aka uncaught), and unknown (see go/adspam-framework for definitions) non-policy invalid traffic; however, since we cannot measure/quantify the unknown category we'll only use defended and undefended as the goal.

GOOG-DOJ-AT-00554716

Strategic intent (medium-term)
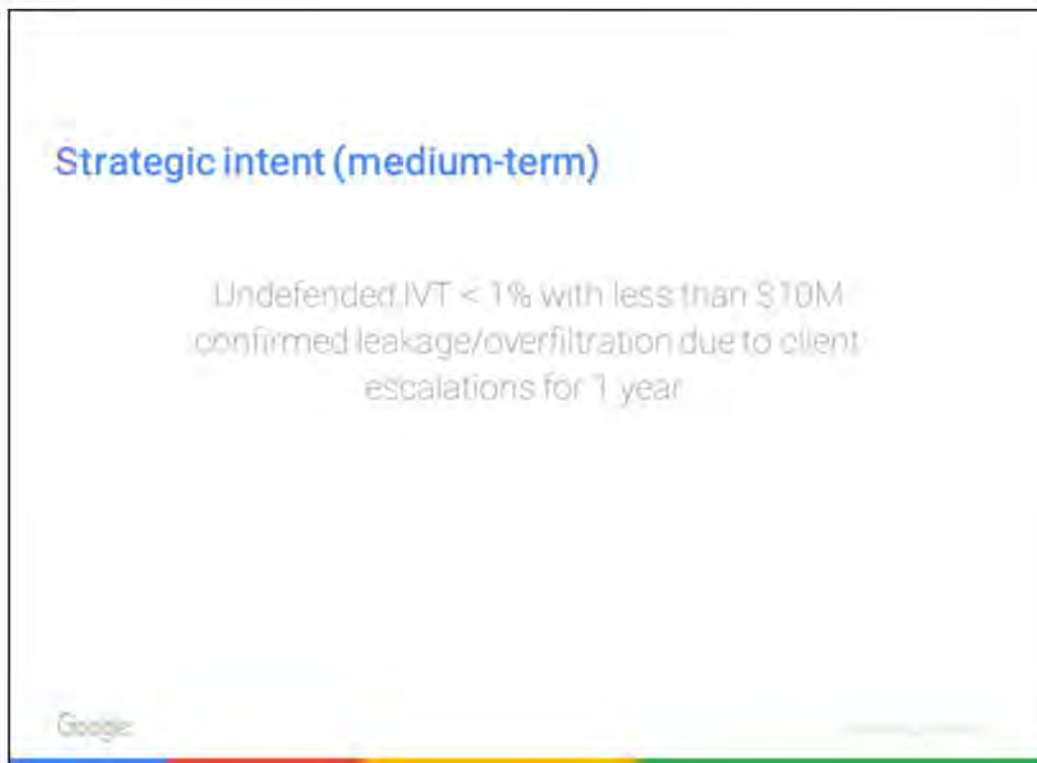
Undefended IVT < 1% with less than $10M
confirmed leakage/overfiltration due to client
escalations for 1 year

Google

Speaker: Per
Mention that we'll do the "work breakdown structure" like for SI - define the next level down
and each sub-team will also define their respective SIs.

GOOG-DOJ-AT-00554717

GOOG-DOJ-AT-00554718

Speaker: Subir

GOOG-DOJ-AT-00554719

DTX-951 Page 16 of 181

AdSpam Eng team structure

AdSpam Eng are organized with five verticals and eight horizontal teams.

VERTICAL TEAMS				
DCLK	GDA	Mobile Apps	Search	Video

HORIZONTAL TEAMS							
AdSpam Infra Core	AdSpam Metrics	AdSpam ML	AdSpam Risk	Botnet Detection	Privacy	User Device and Signals	Trust Graph Infra

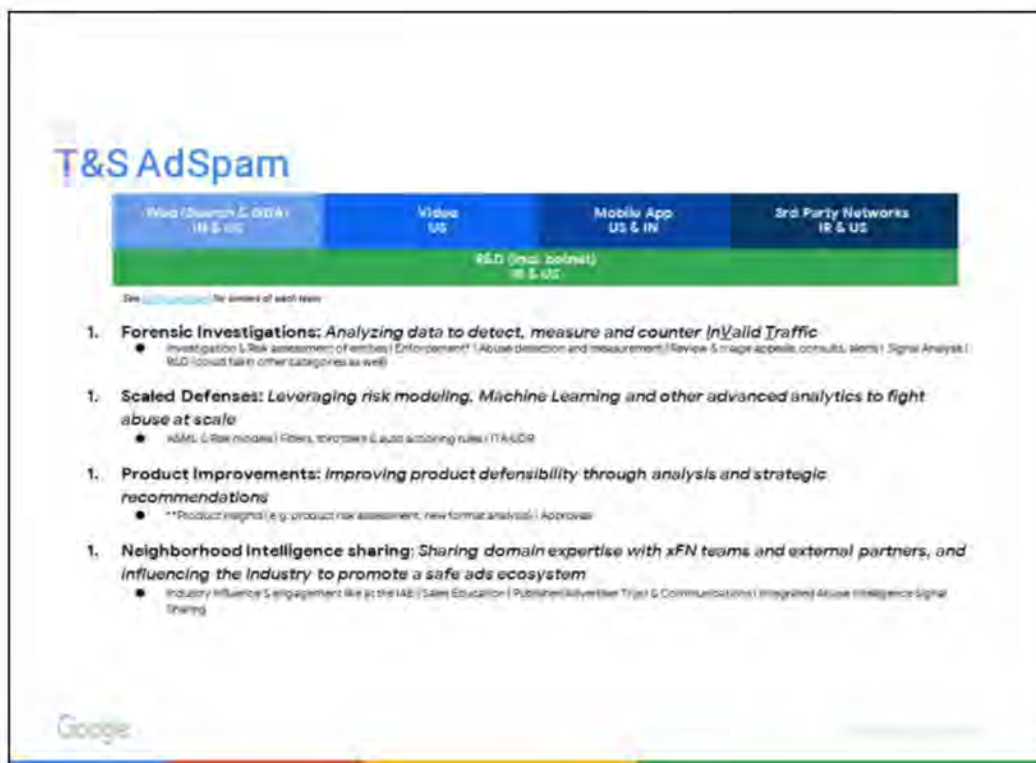See go/adspam-partner-engagement for owners etc. for each team

Google
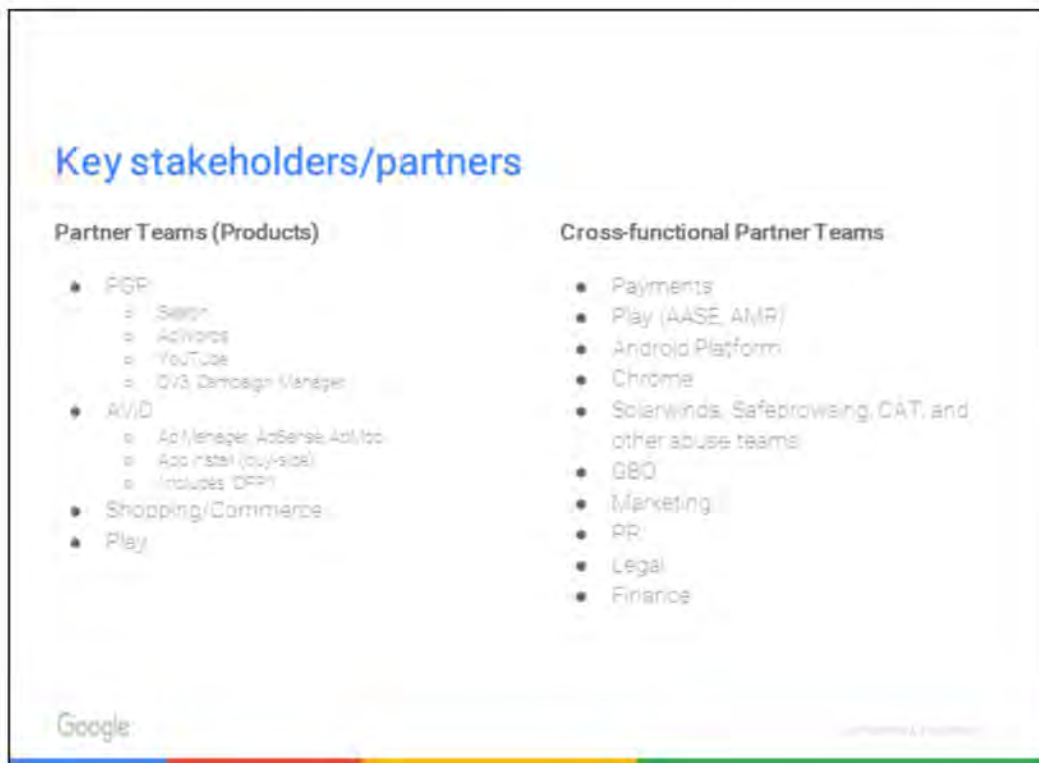
Speaker: Subir

GOOG-DOJ-AT-00554720

Speaker:Puneet
T&S also organizes itself in verticals & horizontals - 4V & 1H. As you can see, there's many similarities how Eng organizes it. Also have project based WGs like Impression spam and a few others.
What T&S does - categories of work...departure from how we used to call Ops and now this new language.
*Enforcement can include: credits | claw back | termination | zombie | suspension | throttle | warning | reinstate | payment hold | sweeps | blacklist maintenance | contract renewals | workflows / comms | Inbound leads: Appeals | Consults | ML | Governator | Throttling | research | SafetyNet | Escalations | alerts | Smart Leads).
** Product insights can include: product risk assessment, product roadmap, product strategy, new format analysis, tools, cases, contract review, pub comm
Add'l details on each category available here.

GOOG-DOJ-AT-00554721

Key stakeholders/partners

Partner Teams (Products)

- PGP
  - Search
  - AdWords
  - YouTube
  - DV3 Campaign Manager
- AViD
  - Ad Manager, AdSense AdMob
  - App install (buy-side)
  - Includes DFP?
- Shopping/Commerce
- Play

Cross-functional Partner Teams

- Payments
- Play (AASE, AMR)
- Android Platform
- Chrome
- Solarwinds, Safebrowsing, CAT, and other abuse teams
- GBO
- Marketing
- PR
- Legal
- Finance

Google

Speaker: Per

GOOG-DOJ-AT-00554722

AdSpam's A&C annual goals recap (1/2)

Build trust in Google's advertising metrics by reducing invalid traffic to advertisers, users and publishers

- [Build Defenses] Reduce AdMob SIVT UDR to below 2% (baseline: ~5.4%) while reducing ad fraud on Google Play by $100M ARR. Projected EOY score: **1.00**

- [Network Health] Improve network health by reducing cost-weighted Account Badness Rate (ABR) on AdSense and AdMob by 50% (currently 11% on AdSense and 6.1 % on AdMob). Projected EOY score:**0.70** (R&D - metrics impacted by COVID)

- [Impression Defenses] Improve impression defenses to reach parity with click defenses for AdMob, AdSense, AdManager, and YouTube (impression based spend and payments account for about $xB ARR). Projected EOY score: **0.70**

- [Botnets]Proactively detect >50% of revenue of botnets (incl. "traditional" mobile botnets) that reach "breakout" size in 2020, and reduce average breakout-to-lead latency by 50% to below 90 days. Projected EOY score: **0.70**

- [Privacy] Launch issuing TrustTokens and have an approved plan for preserving IVT defensibility without dependencies on 3rd party cookies. Projected EOY score: **0.45**

Google

https://docs.google.com/document/d/1vbI8Vb26gVgeubYqJNWqt41kuTcpODVxWglAfc0ansE/edit#

GOOG-DOJ-AT-00554723

DTX-951 Page 20 of 181

AdSpam's A&C annual goals recap (2/2)

(cont.)

- [Metrics] Land continuous monitoring dashboards for Undefended IVT Rate (UDR) for core ads product areas: AdSense, AdX, AdMob, DV360, and [STRETCH] Search, YouTube, and GVP. Projected EOY score: **1.00**

- [Efficiency] Turndown Blitzen and Y deprecated systems to return 480K GCUs. Improve initial leads-to-defense time by 50% (to 3 months) and reduce SWE effort on model validation by 50%. Projected EOY score: **0.75**

- [Signals] Land Adshield 2.0, the next generation of in-app IVT signal collection libraries, and turn down legacy Adshield 1.0 by EOY. Projected EOY score: **0.70**

Block fraud across PAs using Trust Graph

- [Expand coverage] $200M impact through AdSec & Adspam/Play collaboration . X% fraud reduction for one ARES client (Cloud, Gaia, Gmail, or YouTube). Projected EOY score: **0.75**
- [GA] Achieve Trust Graph GA with ASML integration and T&S onboarding. Projected EOY score: **0.60**

Google

GOOG-DOJ-AT-00554724

Speaker Puneet - strategy doc link here
In T&S, we have 7 priorities and aligned with T&S wide 6 pillars.
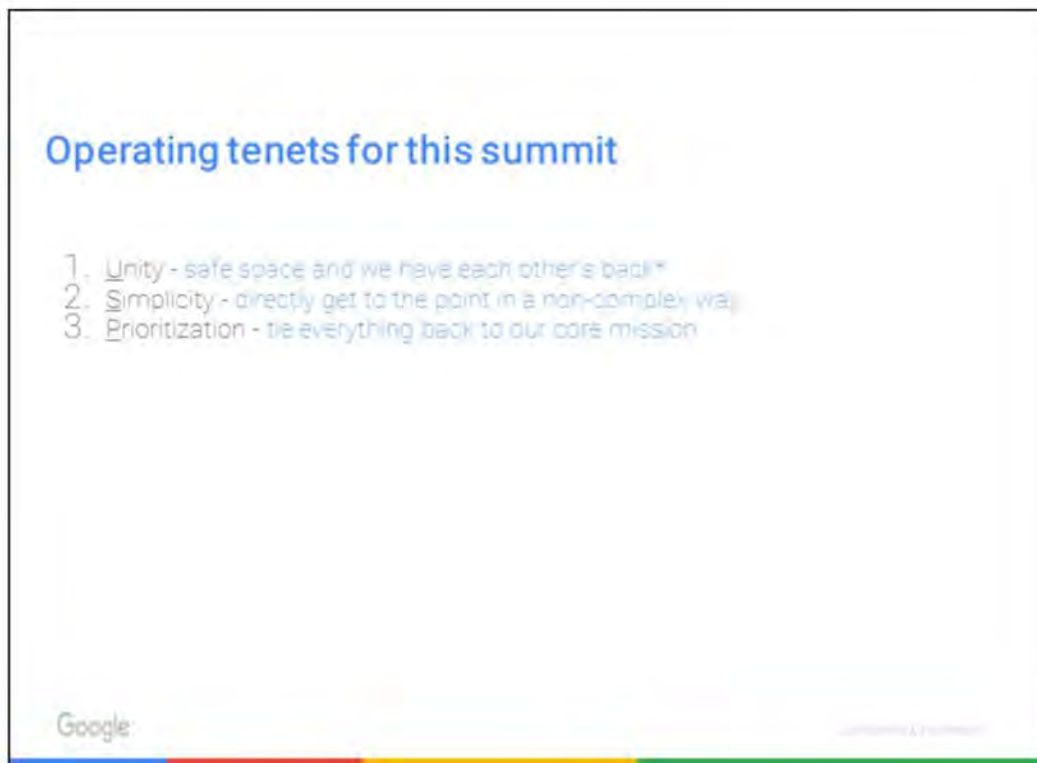
Speaker: Puneet
*avoid sensitive ppl issues

GOOG-DOJ-AT-00554726
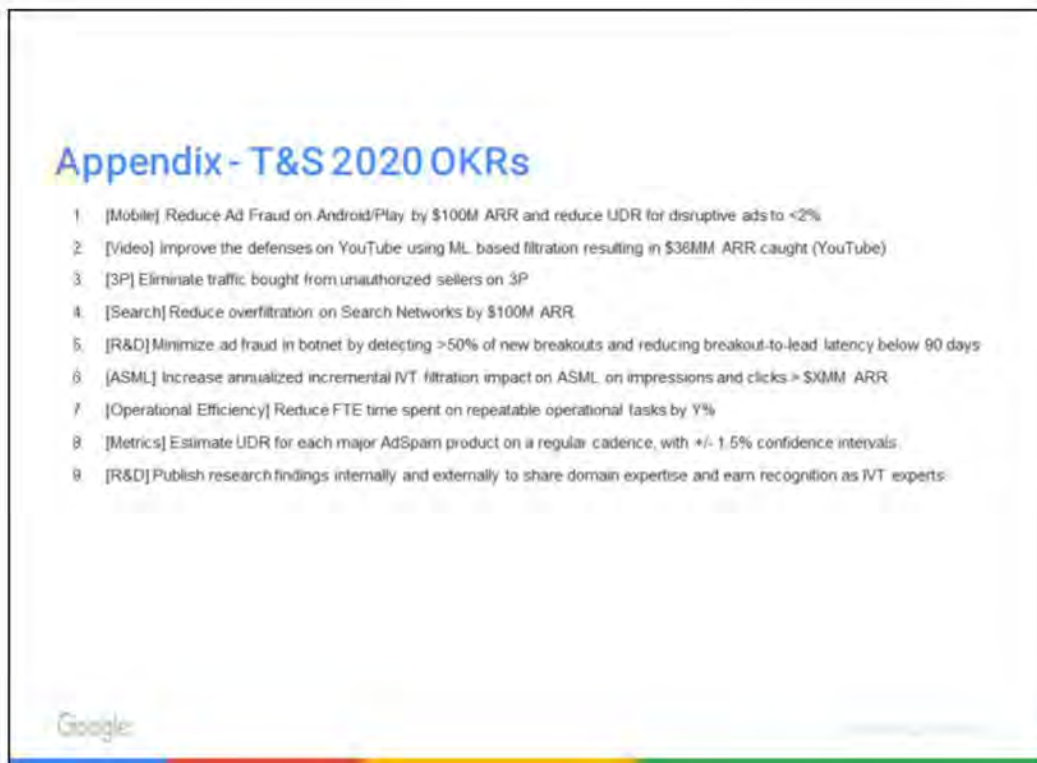
Speaker Puneet
Bonus slide if needed - link to OKRs here quickly skim through the slide as most of it should align with common goals.

DTX-951 Page 25 of 181

Proprietary + Confidential

Break ☕ | 10 mins

PST: 8.20 - 8.30 am
GMT: 4.20 - 4.30 pm
IST: 8.50-9.00 pm

Next session: Planning process

10:00

Google

GOOG-DOJ-AT-00554728

Planning process | 20 mins

PST: 8.30 am
GMT: 4.30 pm
IST: 9.00 pm

Google

GOOG-DOJ-AT-00554729
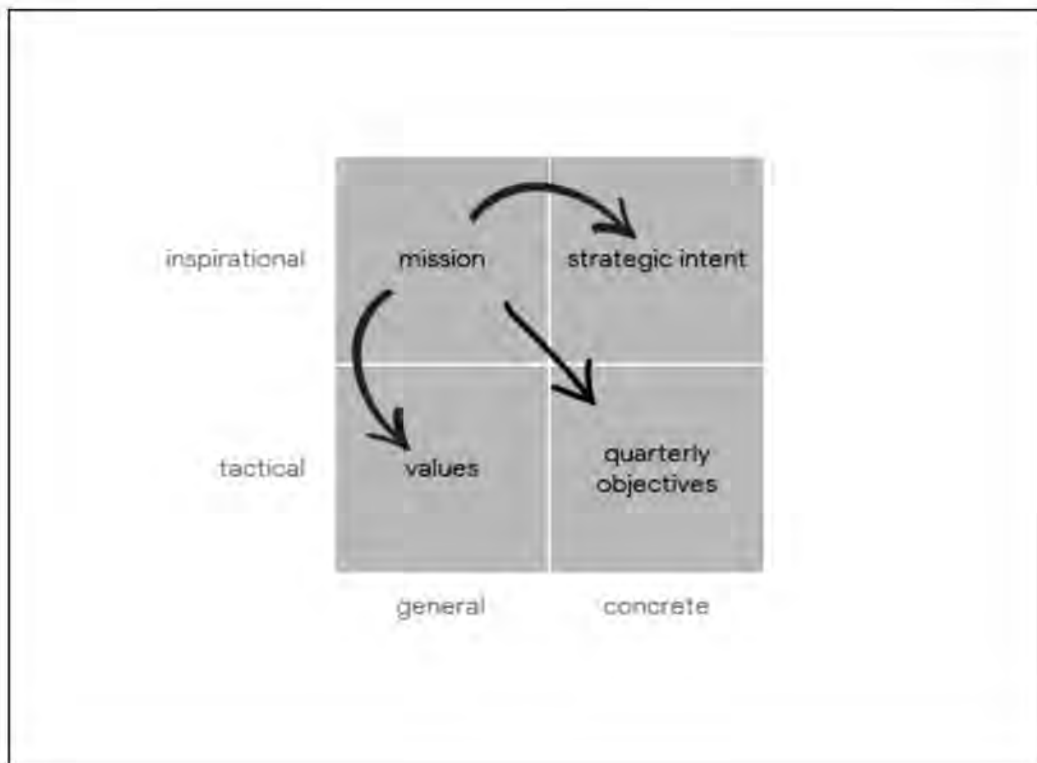
Mission is critical for driving other elements that we need to run the business

Strategic Intent

A declaration of an ambition that concretely describes the desired end-state.

"How will we know when we are done?"

See go/strategic-intent *for a more detailed explanation of strategic intent.*

GOOG-DOJ-AT-00554731

Which one do you think is better?

"Develop digital readiness for the transformation of the 21st Century to modernize Britain and create a more digitally-literate country."

Or

"To get everyone in the U.K. online by the end of 2012."

- Martha Lane Fox, Appointed as UK's Digital Champion

GOOG-DOJ-AT-00554732

Example: AdSpam Sales Enablement

100% of our sales (and support) teams are *autonomously* able to communicate our AdSpam efforts with anyone, anywhere, anytime.

Put differently: zero inbound requests to AdSpam Advocacy XFN team for individual help discussing ad fraud with customers.

GOOG-DOJ-AT-00554733

Planning overview

Strategic/annual planning (once a year)
- Strategy updates
- Strategic Intents (at AdSpam and sub-team levels)
- Annual OKRs (A&C level and sub-team level)

Quarterly OKR planning (every quarter)
- Team OKRs
- AdSpam A&C level OKRs (small subset of key OKRs)

Strategy updates are directional
Strategic intent is more open ended (can span multiple years)
Annual OKRs are more specific and time-bound?

GOOG-DOJ-AT-00554734

"Half year OKR planning"

Suggested: Partially follow a "half-year planning" approach

- Half-year (6 months) planning tasks [in Nov/Dec for H1, in June for H2]
  - Gather input from and align with stakeholders
  - Review new trends/strategic changes/etc
  - Stack-rank projects
- Every quarter planning tasks: "official quarterly OKR planning"
  - Estimate efforts
  - Assign resources
  - Above/below the line decisions
  - Enter into EasyOKR etc

Goal is to reduce the planning overhead in a pragmatic way

GOOG-DOJ-AT-00554735
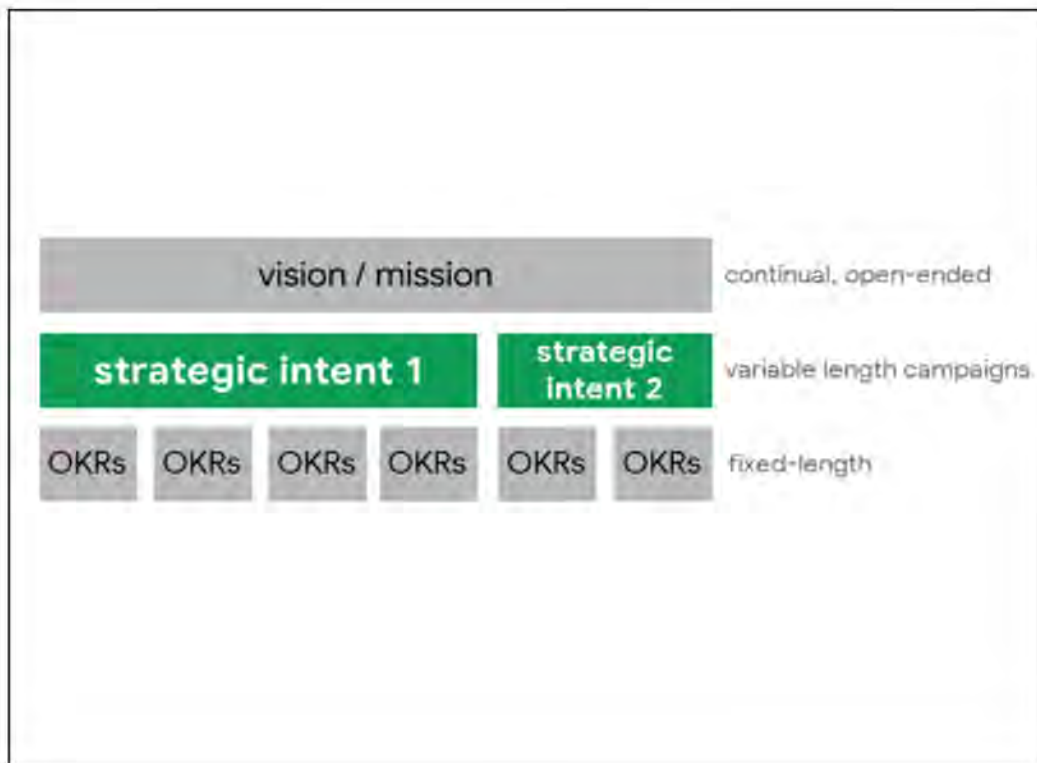
Speaker: Per
While quarterly OKRs are a great way of planning near-term work, the OKRs
approach tends to fall short when it comes to strategic planning and management.
Why? → Because OKRs are bound to arbitrary durations of time. As a result, teams,
organizations, and PAs may find themselves optimizing for the short-term.

GOOG-DOJ-AT-00554736

SI and OKRs at different levels...

GOOG-DOJ-AT-00554737

Speaker: Per

GOOG-DOJ-AT-00554738
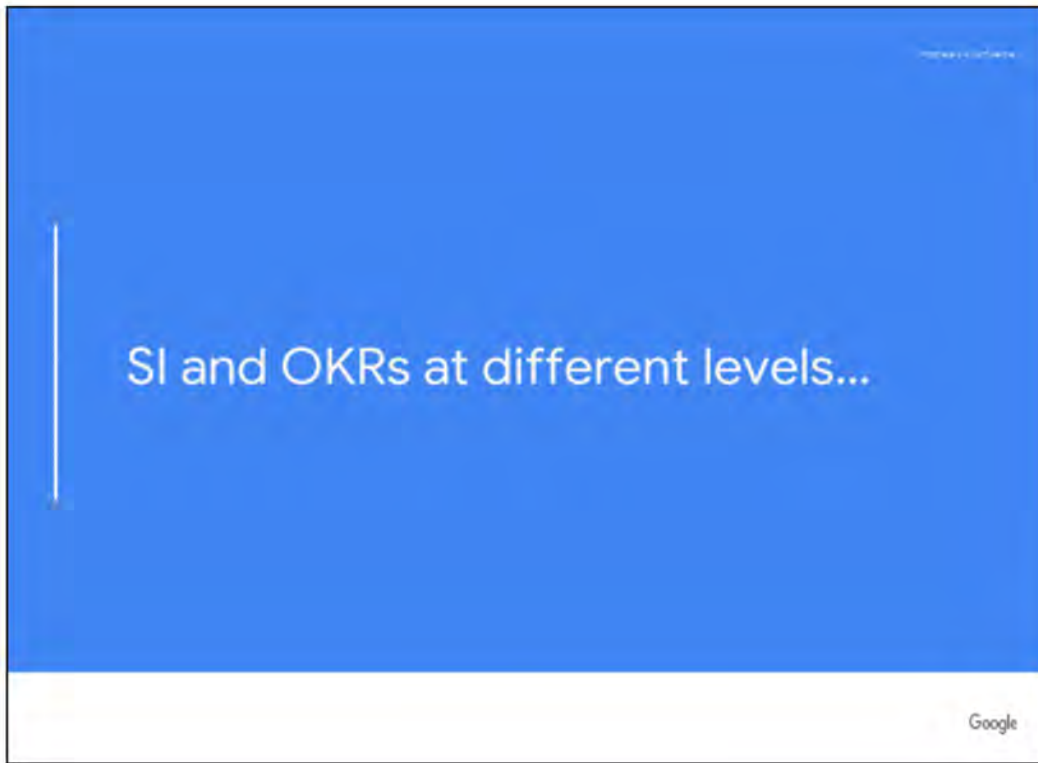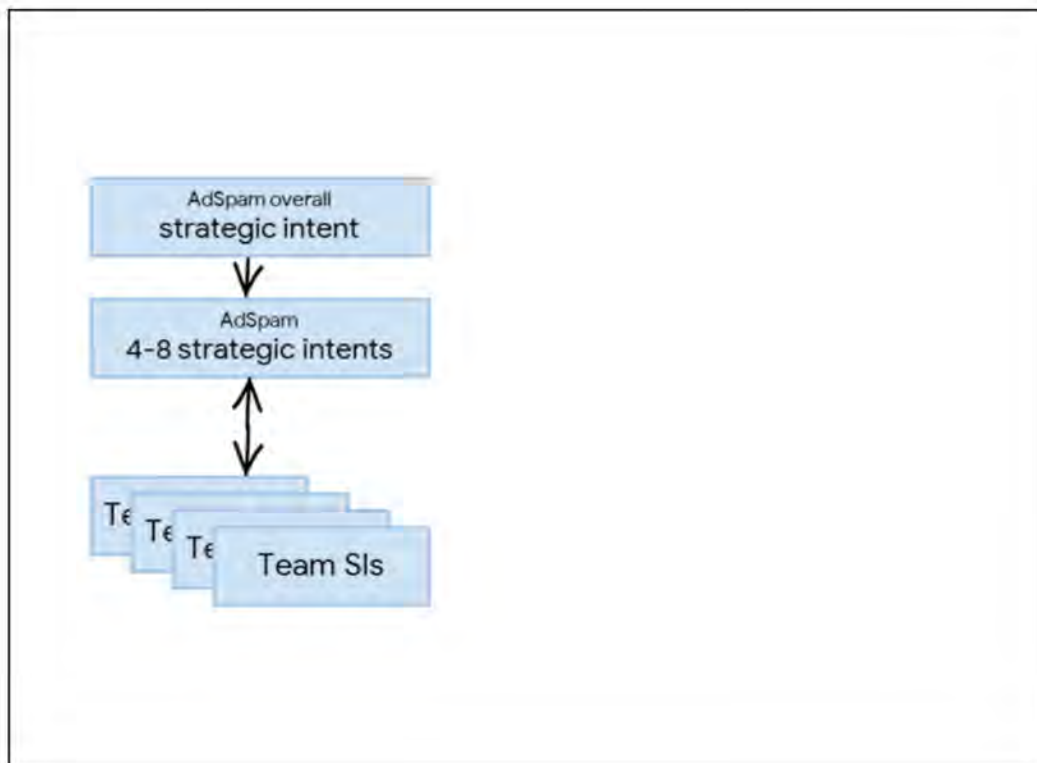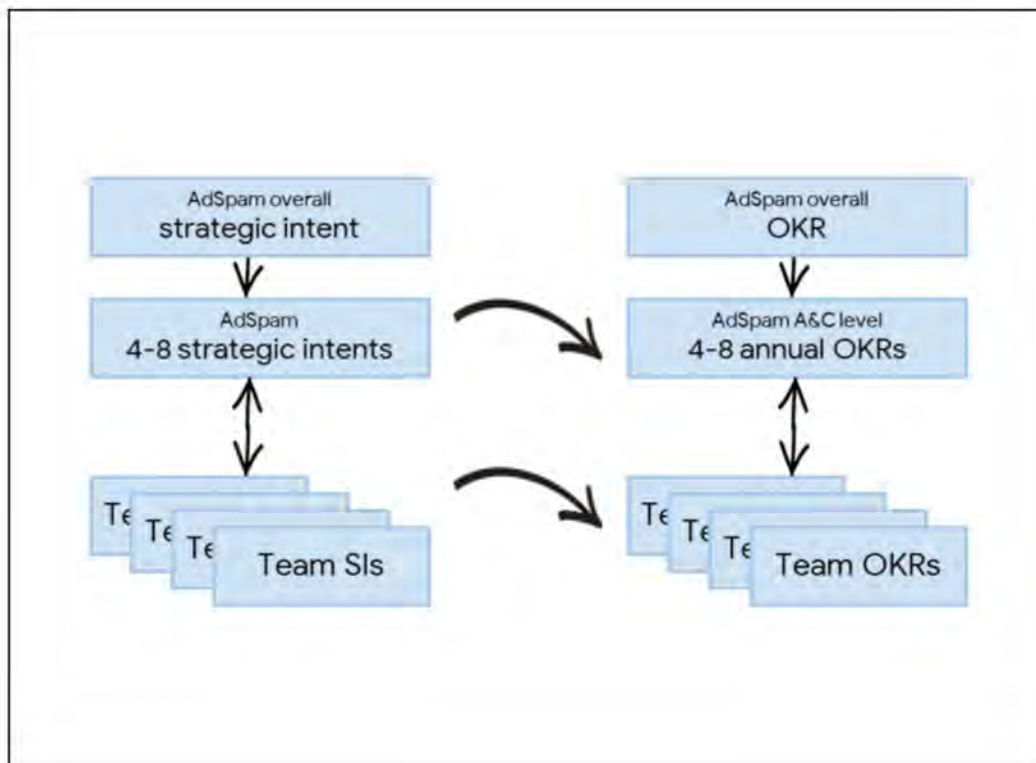
Speaker: Per
Strategic intents inform/drive OKRs
OKRs lead teams to realize a strategic intent.

GOOG-DOJ-AT-00554739

Id	Date	Text
1	06/23/2020 08:45:48	+bjorke@google.com flagging that the relationship should be called out wrt to the Strategic Intents and how they inform/drive the OKRs. Maybe do so verbally or add some text to the arrows. The key point to drive home is that the OKRs lead teams to realize a strategic intent, and not vice versa.

GOOG-DOJ-AT-00554740

Speaker: Per

GOOG-DOJ-AT-00554741

DTX-951 Page 39 of 181

GOOG-DOJ-AT-00554742

Speaker: Aruna

GOOG-DOJ-AT-00554743
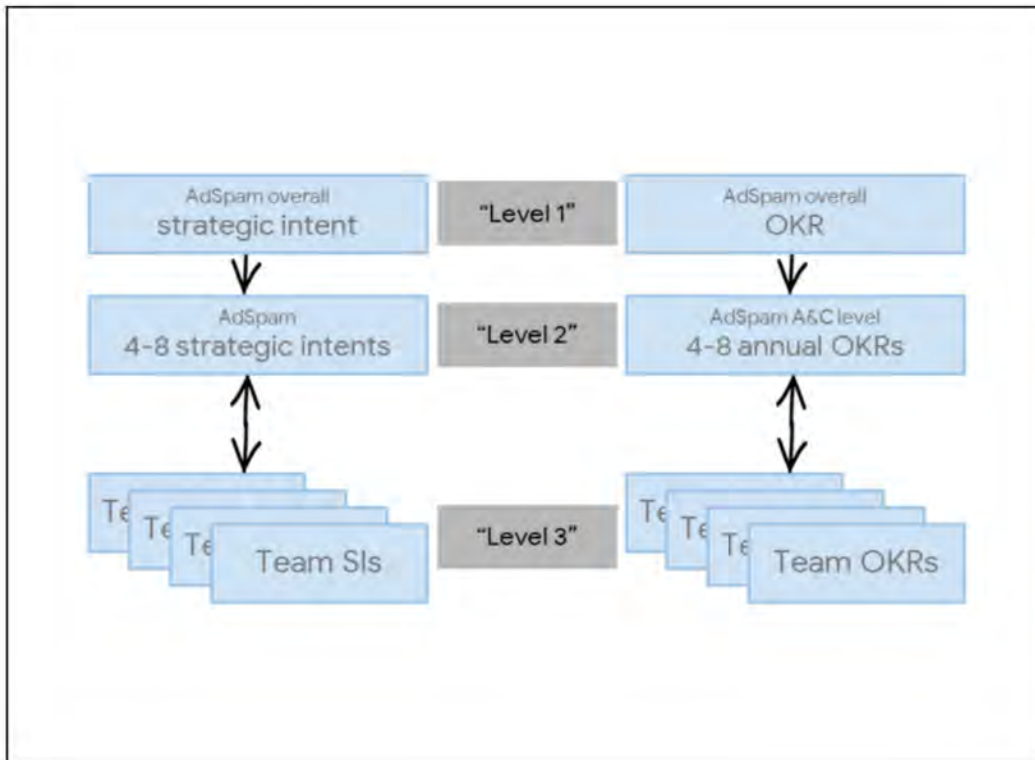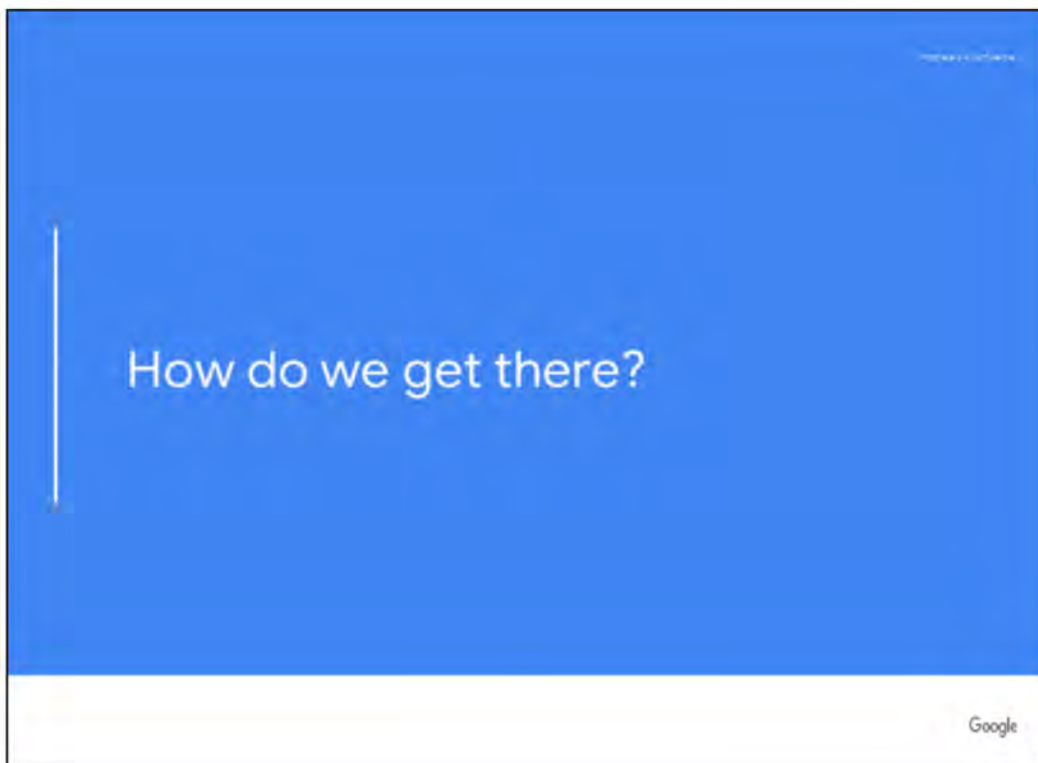
Id	Date	Text
2	06/23/2020 14:44:17	+bjorke@google.com Small nit: Let's rephrase as high-level strategic intents instead of 3-year strategic intents.
1	06/23/2020 14:44:17	This is APaS level slide as it is. The guidance is for 3 years

GOOG-DOJ-AT-00554744
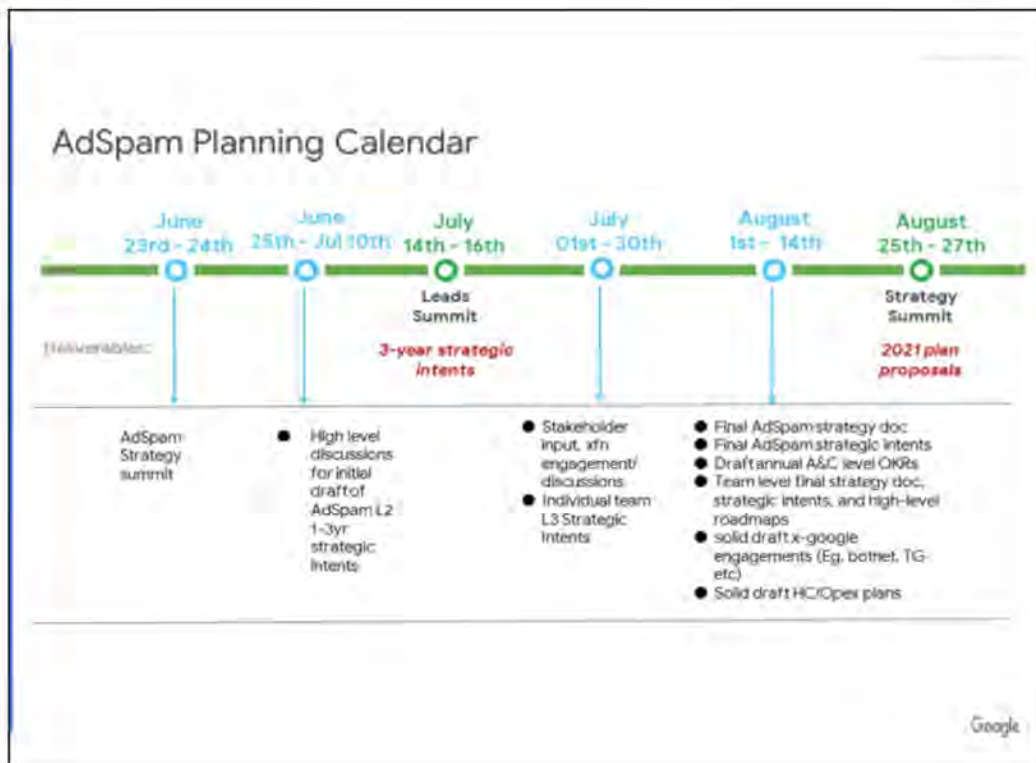
Speaker: Aruna

APaS Slides: https://docs.google.com/presentation/d/1N_D989fGKpVq1cuN0UEtFi-EhzgXmyZbxyTLI5kQD4k/edit#slide=id.g5d3751fd3e_3_53

Draft AdSpam strategy doc
July 14:
Solid draft AdSpam strategic intents (4-7 overall SIs; not sub-team specific)
Team: draft strategy doc, strategic intents (2-5 per team), and high-level roadmap
June/July: Stakeholder input, xfn engagement/discussions, etc.
Aug 25:
Final AdSpam strategy doc
Final AdSpam strategic intents
Draft annual A&C level OKRs
Team level final strategy doc, strategic intents, and high-level roadmaps
solid draft x-google engagements (Eg. botnet, TG etc)
solid draft HC/Opex plans
Nov/Dec:
Finalize annual A&C level OKRs (5-8 OKRs)
Q1 OKR planning
Separately: Q3 OKRs

GOOG-DOJ-AT-00554745

Leads summit
3-year strategic intents
Full doc for pre-read
1-3 slides to guide presentation
X-APaS position papers
1-3 slides to solicit input
No doc due for 7/14-16

Strategy summit
2021 plan proposals
Full doc (draft OKRs, project prioritization, HC / OpEx ask, X-google engagement plans, etc.)
1-3 slides to guide presentation
Final X-APaS position papers
Full doc for pre-read
1-3 slides to guide presentation
Note: full X-APaS position papers are due 8/3, but will be shared / iterated up to the strategy summit

GOOG-DOJ-AT-00554746

Id	Date	Text
3	06/23/2020 09:25:50	+bjorke@google.com same here. Suggest striking 3yr from strategic intents (we don't want to frame as time-bound?)

X-APaS 2021 Position Papers (AdSpam related subset)

Future of our content understanding ML infrastructure: Given the myriad of systems we have across APaS (and PGP/AVID) around content understanding (images, sites, etc), what is our infrastructure strategy to ensure we are not too siloed and reinventing many wheels?
- AdSpam, AI, HUES (shepherd: Rob Malkin)

Security, Privacy, and On-Device: We often see privacy and various safety/security efforts at odds with each other (privacy has a natural tendency to want to reduce signal availability, security often depends on more and more signals). We have dabbled in on-device as a possible path to balance these tradeoffs. Given what we have learned in 2020, what is our 3 year vision around transparency, control, and on-device principles?
- AdSpam, HUES, UX (shepherd: Alejandro)

Team Culture: Improving our team culture and dynamic is a long-term challenge. What can we do short, medium and long term to improve EDII and empower diversity in the team?
- Mike, Tyese, Reid, Karin, Subir, TBD? (shepherd: Tyese)

Google

Speaker: Aruna

GOOG-DOJ-AT-00554748

DTX-951 Page 45 of 181

Id	Date	Text
1	06/23/2020 23:49:35	@aruna@google.com What's Alejandro's ldap? Should we be engaging with the on-device x-apas 2021 position paper? _Reassigned to Aruna Kommu_
2	06/23/2020 23:49:35	aborgia , FYI, Subir mentioned in the summit that he will connect the right group to Alejandro.

GOOG-DOJ-AT-00554749

Building for the future

One-time efforts
- Platform investments
- Infra/tool migrations (what we know of: Zoomout | New: TBD)
- Others?

Recurring efforts
- Engineering and product excellence efforts
- MRC (2 or so audits per year)
- SOX (every year)
- Resource Planning (yearly & quarterly)

Reminder: Be empathetic and supportive of asks across sub-teams within AdSpam

Google

Speaker: Aruna

GOOG-DOJ-AT-00554750

GOOG-DOJ-AT-00554751
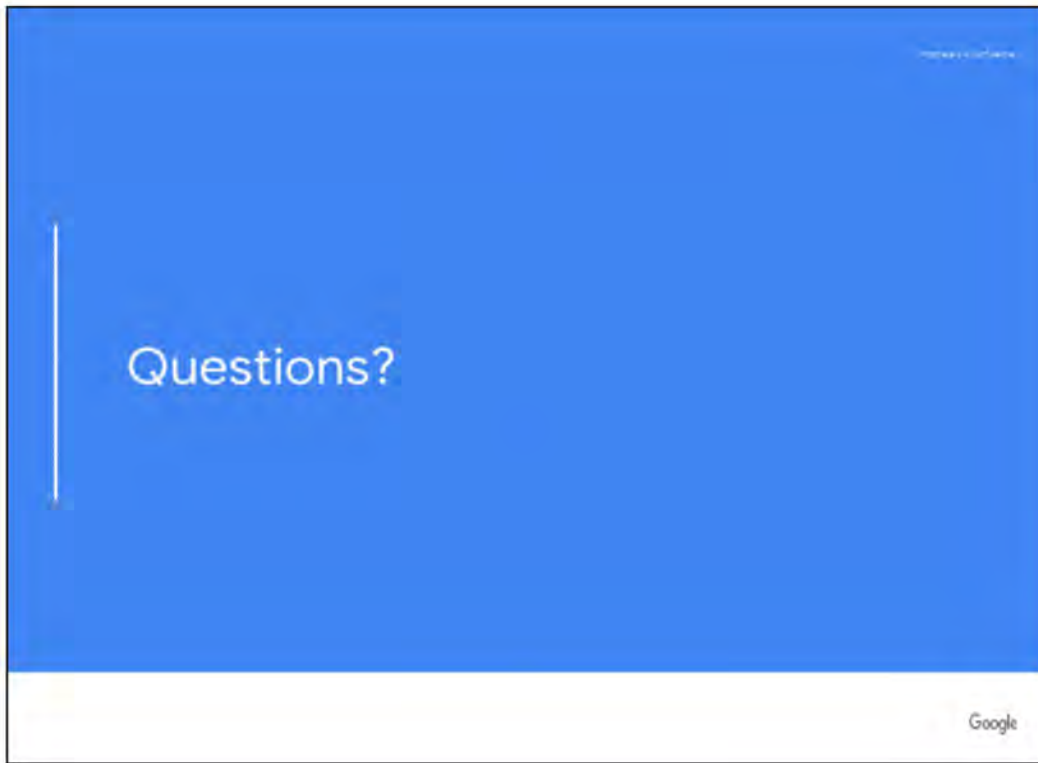
Future of AdSpam Infra | 60 mins
PST: 8.50 am
GMT: 4.50 pm
IST: 9.20 pm

GOOG-DOJ-AT-00554752

Outline

- Enforcement and training – prod models, TPU training, prebid and pre-budget, teacher/student training/serving (akademia), launch automation, experiments (rasta integration), lower latency policy
- Turndowns
- Simplifying signal ingestion and data governance.
- Standardizing downstream spam processing – credits, spam/unspam/retractions
- Machine constraints
- Preparing for Privacy, on-device

GOOG-DOJ-AT-00554753

State of AdSpam Platforms
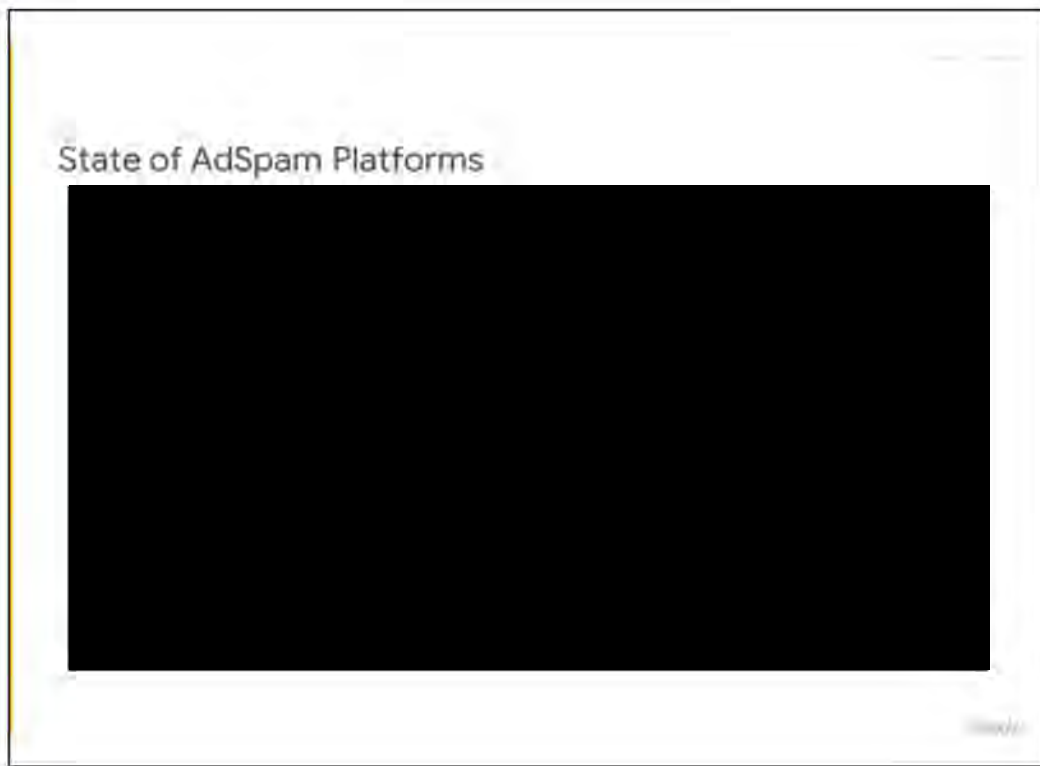
Famous picture that we use to scare Nooglers in AdSpam. At times this has also helped in convincing senior leadership to do some painful investments.
But instead of focusing on the complexity I want to emphasize the strengths.

Flexibility

- **Training and enforcement** at different feature rich environments - prebid vs post serve.
- **Training options** - aggregation based rules (masonite), weak labellers (LGP/drybell), DNNs (Adbrain)
- **Enforcement options at different timescales** - prebid, pre-budget, post serve, credits/debits
- **Protecting advertiser budgets & users** – pre-bid, pre-budget
- **Enforcement of different IVT** - policy and non-policy.
- **Correction of over/under filtrations** post facto.

Biggest strength is flexibility.
Training & enforcement - joined logs vs just the bare QEM or just the bare CEM
Enforcement options at different timescales - different options have different impact
on the business and our advertisers; These also come with tradeoffs around what you
can train with.
Protecting advertiser budgets & users against different kinds of spam

Scaling the platforms - Highlights

- **AsPol (AdSpam Policy)** - The new policy rule enforcement system.
- **Memento** - The new stateless enforcement system.
- **RTAS on all stacks** - CAT2, Click pingback, Call tracking, Viral, Search, DFP, Xbid.
- **ASML enforcement** at click ping back and prebid in addition to post-serve.
- **Teacher/Student training/enforcement** capabilities in ASML.
- **Richer unsupervised techniques** - Representation learning, Active learning, Label propagation, GCN heterogeneous graph processing.
- **Mendel and Rasta integrations** for streamlined experiments.

Google

AsPol - streaming grouping and aggregation

GOOG-DOJ-AT-00554756

Scaling the platforms - Challenges

- **Many more systems** than maintainers - fragmented know-how, monitoring and tooling.

- **High cost** of maintenance - leading to escalations.

- **Cost of tech debt and mandates** keeps increasing.

- **Difficult to reason about** - capabilities, impact, coverage.

- **Inability to invest** in solving other issues - signal ingestion, portability etc.

One of the ways in which we are trying to tackle these challenges is by putting more wood behind fewer arrows and limiting our focus on fewer systems - systems that cover all use cases (policy, non-policy, different enforcement options, different training options) which are built on modern sustainable architectures and technology.

To that end we have an A&c level goal to turn down blitzen which happens to be one of the largest and complicated system in our fleet. Back in 2018 we did a CM that stabilized Blitzen but the cracks are again beginning to show.

GOOG-DOJ-AT-00554757

Scaling the platforms - Blitzen Turndowns
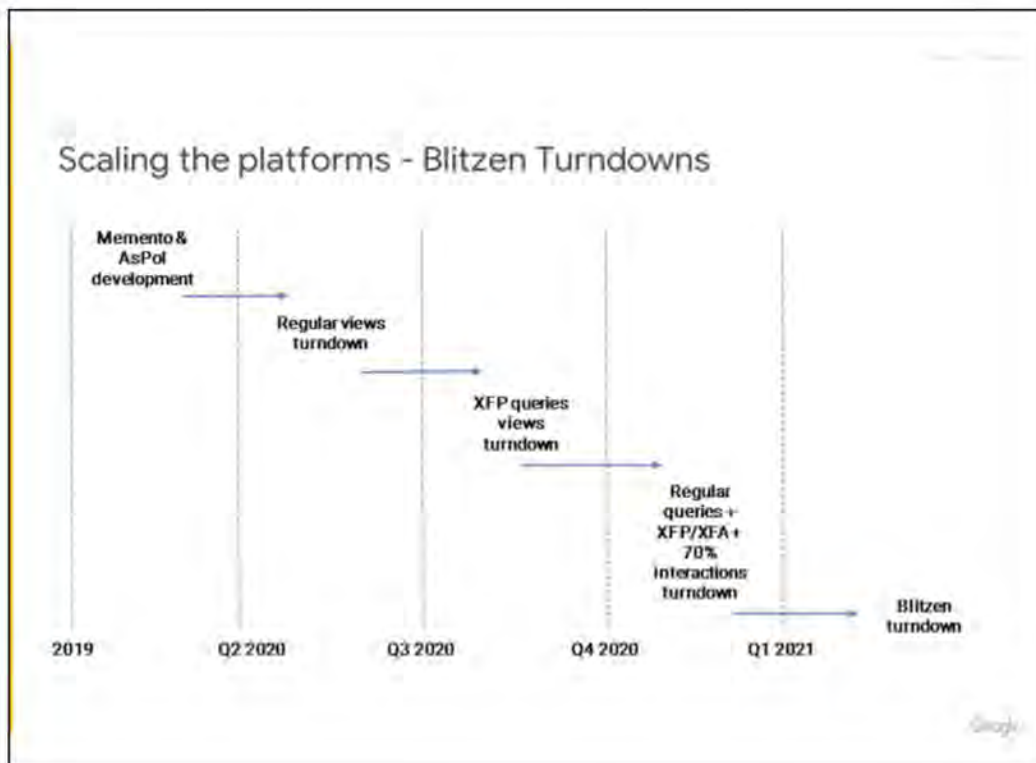
Challenges:
- Blitzen non-determinism
- Blitzen lack of past spam capabilities
- No portability
- Incre/decre cannot be measured with metrics

GOOG-DOJ-AT-00554758

Id	Date	Text
1	06/23/2020 12:08:41	@jfmatthews@google.com @vram@google.com sgty?
1	06/23/2020 12:08:41	Q4 seems very crammed given that its a short quarter. XFP/XFA = 7 pipelines (given that xfp views should get done in Q3).

GOOG-DOJ-AT-00554759

Scaling the platforms - Unit Turndowns

Vertical	Unit	Ongoing work	Unlaunch ETA
Search	Dist	Shadow mode	Q3
	Google	Slim review	Q3
	External YJ	pCC and LGP models in soft launch	Q3
	AFS	LGP models in development	Q3
GDA	:	pXY models in development	Q3
Mobile	-	pXY, pTouchDuration	Q3
Video	-	pXY	Q3
	Taco/TVI	Scoping; Not started	Q3/Q4

- Largely making good progress; search &gda -- well defended on asml; mobile & video - pxy;
- unlaunches are followed by shadow mode experiments for a quarter to study if the existing defenses are helping capture a unique fingerprint of spam.

- Shoutout to verticals and TnS - Cross team effort to streamline our defenses and simplify our systems.

- So this is today and how we are walking down the path that we set out in 2018/2019. But whats in store for the future. Beyond stabilizing and simplification we want to invest in areas that can increase AdSpam's impact and improve productivity.

GOOG-DOJ-AT-00554760

Id	Date	Text
2	06/23/2020 16:47:44	@kendrickb@google.com @jfmatthews@google.com does this look fine. I tried to compile info from the status spreadsheet and Kendrick's doc.
1	06/23/2020 16:47:44	For Afs, something like "sprint to develop PCC and LGP models in July" is the current status. Video also has ongoing, required work to launch expanded PCC models.

GOOG-DOJ-AT-00554761

Scaling the Platforms - Today & Beyond

Signal management

- Signal acquisition and plumbing continues to be a large % of verticals workload.

- Standardize production data stores - Woodshed & TG

- Standardize production frameworks for data ingestion - operationally managed workloads - separation of infra failures and data failures.

- Standardize data governance - data dependency tracking, root cause analysis, reduce operational overhead.

- Support easy plumbing and PD analysis of experimental data.

We want you to be able to not worry about how the data is sourced; you should be responsible for validation of sanity of data and the business logic that makes use of this data but everything else should be automated for you.

GOOG-DOJ-AT-00554762

Scaling the Platforms – Today & Beyond

Standardizing AdSpam's role in corrections of Ads

- Does AdSpam's charter include generic corrections in Ads or only IVT corrections?

- Formalize the correction API for Ads – Matcha as a matching API, MaaS for matching, spam/unspam Vs retraction/restatements for correcting.
  - What do advertisers/publishers see?
  - What do downstream teams regard as IVT?

- Move all core stats correction into Conflux.
  - AdSpam only produces spam. Credits/Debits Vs in-month correction all aligned with downstream month close boundaries.

This is a broad area that goes beyond Adspam but it is very relevant for our day to day operations. AdSpam is in the business of identify and enforcing IVT - both policy and non-policy. But there have been several incidents in the past where AdSpam annotations are used for correcting experiments that have gone wrong. There are new use cases emerging where Ads looks at AdSpam as a way to correct stats/advertiser payouts.

There are several reasons for this - we have a popular set of APIs and services for picking the relevant events that need to be corrected and we have the systems to produce the annotations that have the intended impact. But are these the correction annotations?

Beyond standardizing and clarifying our role we also want separation of concerns - AdSpam should not be in the business of monetizing IVT/correctons - not an area where our strengths are and we are not properly setup to handle this charter.

GOOG-DOJ-AT-00554763

Scaling the Platforms – Today & Beyond

Portability and Upstream defenses

- Toolkit for portability of defenses at different timescales - prebid, pre-budget, post-serve.
- Automatic monitoring, validation, skew detection and other consistency checks.
- Consistent tooling and evaluation capabilities.
  - Helps protect advertiser budgets.
  - Critical for Real time stats.

Business attribution

- Build visibility and attribution as a first class use case in AdSpam.

  - Critical to understand impact of our systems
  - Critical for corrections during escalations.

GOOG-DOJ-AT-00554764

DTX-951 Page 61 of 181

Scaling the Platforms – Today & Beyond

Privacy

- One of the biggest challenges facing AdSpam today.

- Expected to at least 2-3x the number of variants of filters.

- Challenges

  - Scalable what-if analysis and simulation.
  - Scaling our defenses for the long tail.
  - Ease of rollouts/rollbacks.
  - Automatic monitoring and consistency checks.
  - Time bound deliverables.

- Lack of clarity on interplay of on-device learning - is this complimentary to the existing privacy efforts or an additional requirement?

Google

GOOG-DOJ-AT-00554765

DTX-951 Page 62 of 181

Machines

- Machine budgets continue to tighten.

- Scrutiny on all dimensions – GCUs, RAM, IO etc.

- Adhoc requests and annual machine budgets changes are going to attract attention.

- **Suggestions**

  - ○ Plan ahead.
  - ○ Align on fewer systems.
  - ○ Weigh filtration impact against resources.
    - ■ Can a 10x cheaper model get you 90% of the impact?

Google
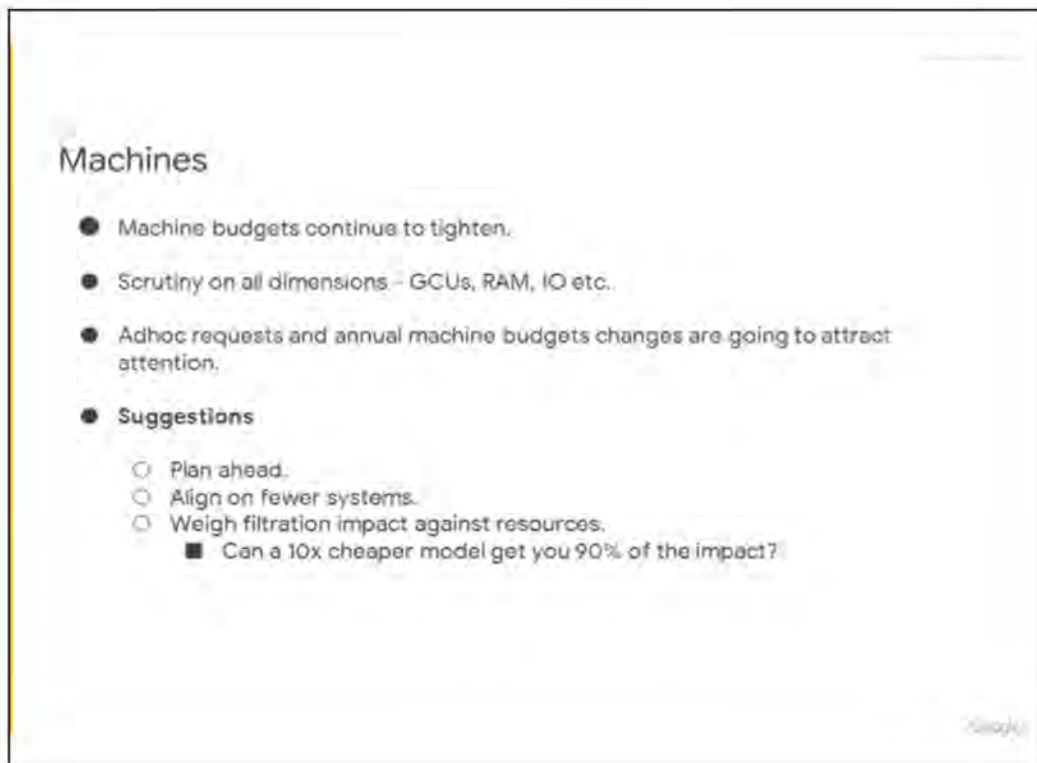
And lastly a word from our sponsors - capital engineering

Ex. display doesn't serve the entire corpus of 300+M ads - only 20M at any time.

GOOG-DOJ-AT-00554766

Summary: 2018 goals vs 2020 reality
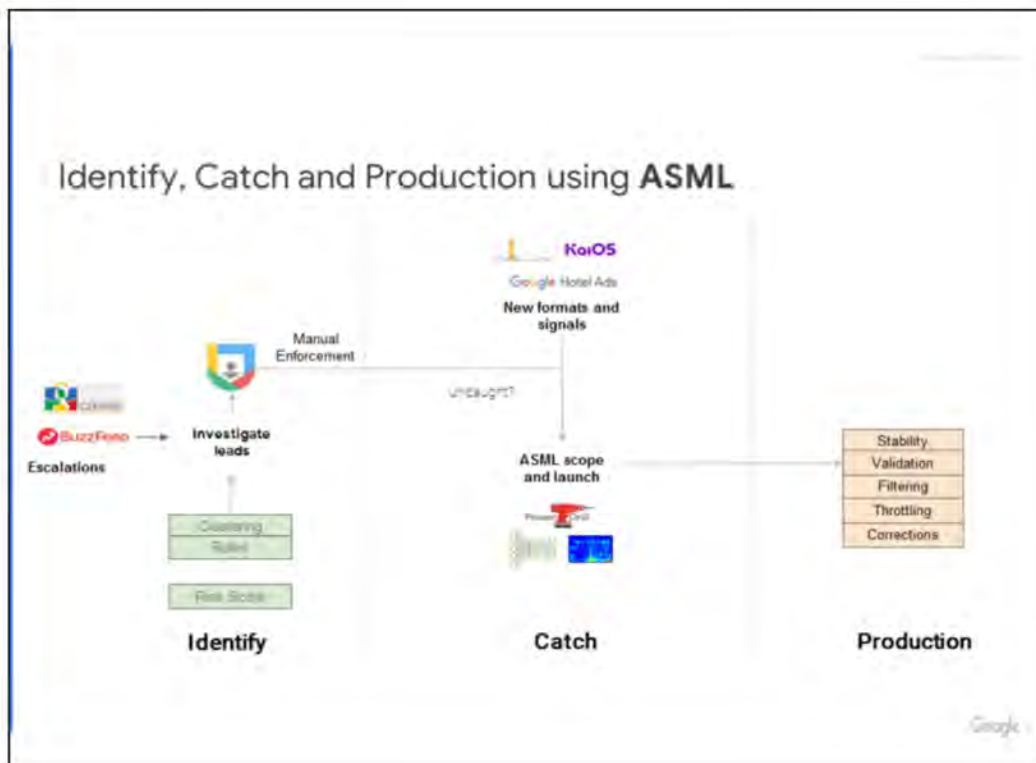
		Q1 2020 Status
Coverage	Be the AdSpam solution for 95% non-policy spam	97%

Faster defenses

	Q1 2020 Status
• 90% of spam caught seconds, protecting advertiser budgets	93% pre-budget
• Identify and catch uncaught spam 3X faster	3X faster, $1.2B incremental
• 3 week launch from spam leak discovery	3 months

Production stability

	Q1 2020 Status
• Precision guarantee using online quality monitoring	GoldStone monitoring
• SLA adherence	4 escalations past year
• <2 SWE/Q oncall overhead	1 SWE/Q average

Delight the user

	Q1 2020 Status
• > 4/5 user rating	4/5
• < 12 hour model iteration	10 hour

Google

GOOG-DOJ-AT-00554767

Identify, Catch and Production using **ASML**

GOOG-DOJ-AT-00554768

Accelerating **Identification** using Entity Insights

Automatically annotate each Entity with insights using traffic, content, entity signals

Anomaly score: Scores indicating badness with signal-based reasoning

Related entities: Entity rings and clusters, entities with same signal fingerprints

Related badness: Related to existing or past attack?

Active learning lift: How much incremental spam if labeled for MLT

2020 Q2-Q3: Demonstrate feasibility

2020 Q3-Q4: Productionize as part of filter and validation launches

2021 proposal:
- H1: GA on all verticals
- H2: integrate with TnS review tools for **instantaneous** exploration

Google

GOOG-DOJ-AT-00554769

Catch: Continuously learn from enforcements

3 Week launch from spam leak discovery | 3 months

New Leads

TnS Review systems — Enforcements — Credits Manual Blacklists

Scope and launch ~3-6 months

"Having enforced an entity in the past, can we ensure this attack is automatically filtered?"

GOOG-DOJ-AT-00554770

GOOG-DOJ-AT-00554772
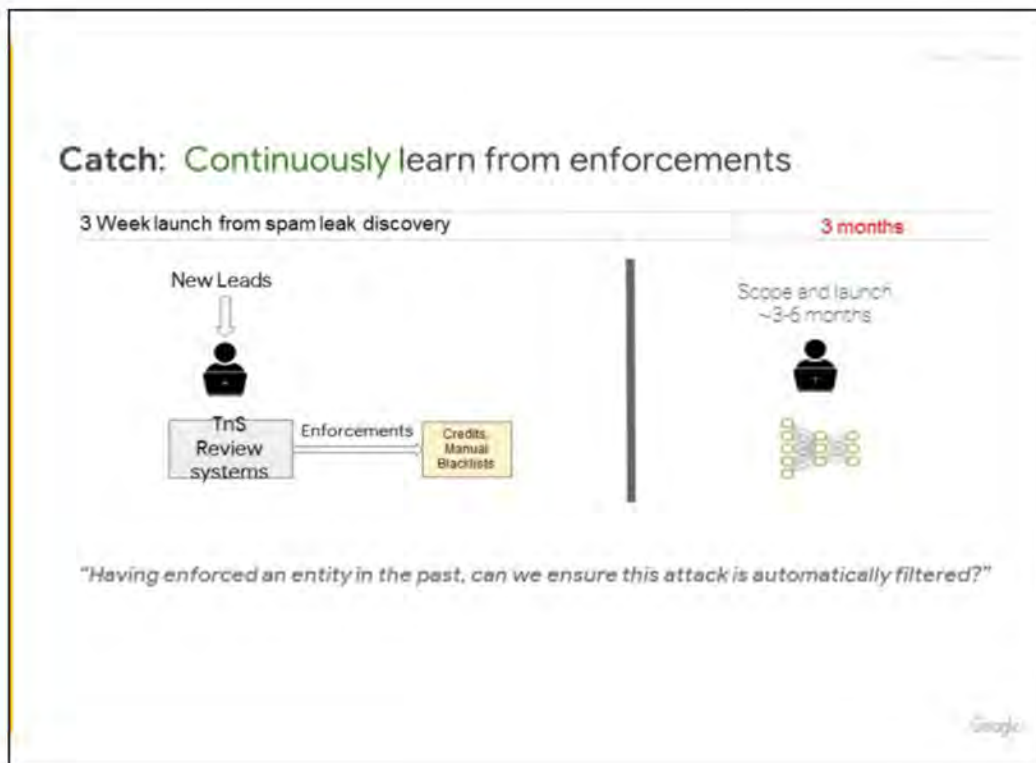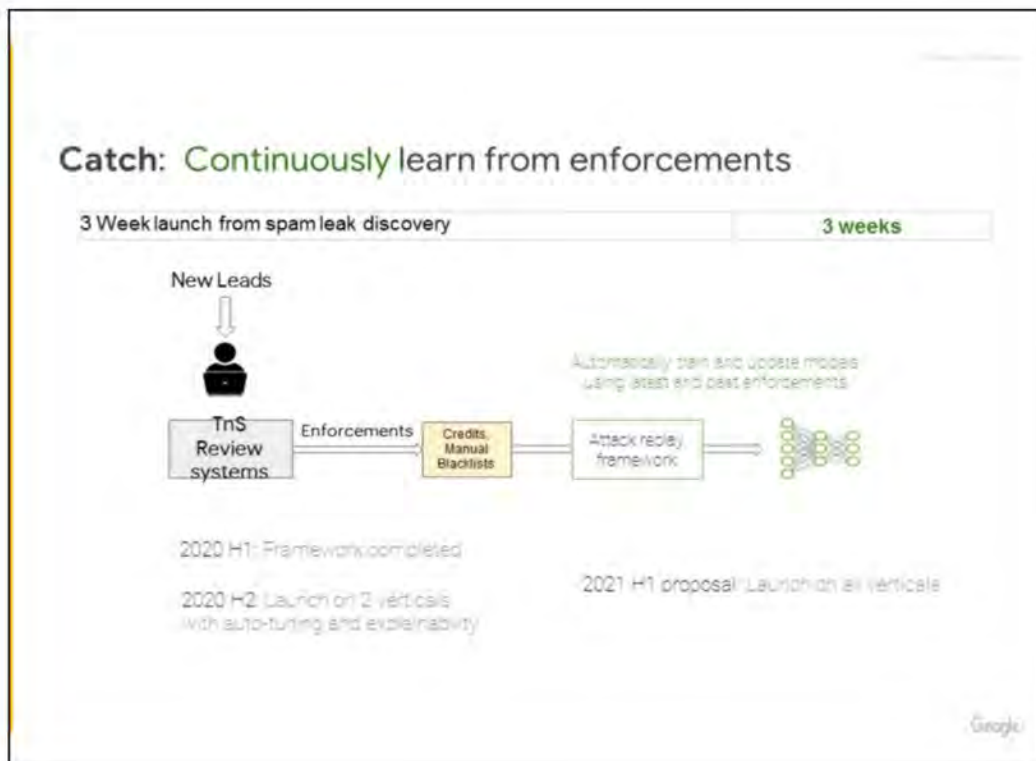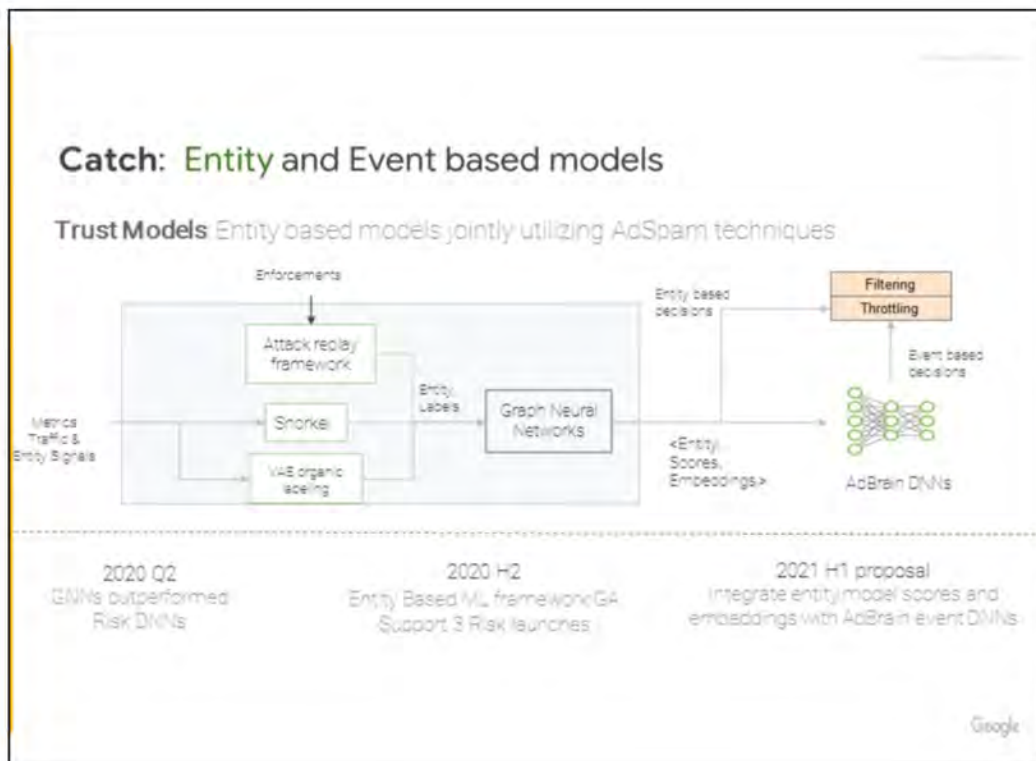
Accelerating signal utilization

"Make it easy to determine if a signal is useful, utilization will follow"

2019: Manual signal and feature engineering in LGP

2020 H1: Launched VAEs to automatically determine signal buckets weights combinations and importance

2020 H2: A/B experimentation framework. GNNs to utilize both traffic and **entity signals**

We can accelerate a lot more in 2021:

Signal and rule suggestion framework
- Rank order any set of signals based on potential spam importance
- Suggest rules based on signals to generate ground truth

Google

GOOG-DOJ-AT-00554773

DTX-951 Page 70 of 181

GOOG-DOJ-AT-00554774

DTX-951 Page 71 of 181

Monitoring Gaps

2019 Q4:

- GoldStone monitoring limited to ASML
- Handful of metrics used in quality monitoring
- No SFRC. Manual checklists monitoring
- Quantity monitoring spikes difficult to explain
- New launches require monitoring configured

2020 goal:

*"Any manual or automated filter is **automatically** quality and quantity monitored with slice-level attribution and 50% actionability"*

GOOG-DOJ-AT-00554776

Monitoring Solution

Gaps	2020H1	2020H2
GoldStone monitoring limited to ASML.	Demonstrate usefulness of GoldStone monitoring on Search and GDA filters	GoldStone to monitor all AdSpam filtration
Handful of metrics used in quality monitoring.	GoldStone integrated with ASTM. Currently uses 90 metrics	Add all possible metrics (~120) integrate Botnets metrics
No SPRC. Manual blacklists monitoring.		Deploy GoldStone and quantity monitoring for blacklist monitoring
Quantity monitoring spikes difficult to explain.	Proof of concept with Graph Mining attributing slices to quantity spikes	Productionize and deploy alongside quantity monitoring
New launches require monitoring configuration changes	Demonstrate Ensemble Metric is adequate to monitor quality of all Search and GDA filters	Automatically monitor **all** models as soon as they hit live traffic

Google

GOOG-DOJ-AT-00554777

Id	Date	Text	
1	06/22/2020 18:34:23	+ykzhu@google.com please check if this aligns with our plans. _Assigned to Yong-Kang Zhu_	Proprietary + Confidential

GOOG-DOJ-AT-00554778

DTX-951 Page 75 of 181

GOOG-DOJ-AT-00554780

Metrics | 30 mins

PST: 10.00 am
GMT: 6.00 pm
IST: 10.30 pm

Speaker: Zack

Ads OKR: Land continuous monitoring dashboards for Undefended IVT Rate (UDR) for core ads product areas: AdSense, AdX, AdMob, DV360, and [STRETCH] Search, YouTube, and GVP.

Speaker: Andrew

Signal Metrics - ASTM (AdSpam Traffic Metrics)

A standardized library of signals and derived metrics:
- Metric definitions are centrally defined implemented, tested, and productionized
- Easily configurable
- Nearly instant
  - No more SQLP → PD slog
- Shared across the team
- Dragged and dropped via Plx Explorer

"Write once, run everywhere immediately"

2020 H1	2020 H2	2021 proposal
Integrated with LGP, GoldStone TG Assistant. 90+ metrics added Complex metric (e.g., CG) infra added	Drag and drop via Plx Explorer Integrate with TG Storage Onboard Botnets pipelines Autotuning Infra (non-CG)	Retire/onboard all classic pipelines Integrate with AdBrain Integrate with TnS review tools

Google

Speaker: Souvik

GOOG-DOJ-AT-00554784

DTX-951 Page 81 of 181

Speaker: Souvik

Speaker: Souvik

GOOG-DOJ-AT-00554787

DTX-951 Page 84 of 181

DTX-951 Page 85 of 181

GOOG-DOJ-AT-00554788

GOOG-DOJ-AT-00554789

GOOG-DOJ-AT-00554790

Two Primary Goals

Prevent ability to track users across sites (web only)

Provide user transparency, choice, and control

Google

GOOG-DOJ-AT-00554791

Major Privacy Initiatives

- **Web**
  - ○ Chrome's Potassium: Prevent ability to track users across sites (Privacy Sandbox)
  - ○ Ads' Newton: User transparency, choice, and control (opt in/out, who is collecting, delete)

- **Mobile apps**
  - ○ Anning: User transparency, choice, and control (opt in/out, who is collecting, delete)
  - ○ Event Attestation (aka "Secure ADID"): Core technology to make Anning work
  - ○ On Device Ads: "No data should leave your device"

- **Consent regulations leading to cookieless ads (ePrivacy etc.) (web + mobile)**
  - ○ No ads cookie/ADID etc. without user consent (currently in EU)

Google

GOOG-DOJ-AT-00554792

What Does This Mean For AdSpam?

- **Privacy for web**: Chrome's "Potassium" + Ads' "Newton" projects
  - How can we minimize the loss of defenses with no 3P Cookies + Anti-Covert Tracking?

- **Privacy for mobile apps**:
  - Anning + Event Attestation: WebViews vs In-App Browsers
    - Different defenses for Display/Video ad traffic within WebViews in Anning?
  - On Device Ads
    - No more logging of individual events (e.g. no more QEM, CEM)

- Web + mobile: **Consent regulations leading to cookieless ads** (ePrivacy etc.)
  - How do we handle loss of 1P/3P cookies/AAID with ePrivacy?

Google

GOOG-DOJ-AT-00554793

GOOG-DOJ-AT-00554794

Chrome - Today

	youtube.com	google.com Search Results	publisher.com Ad	advertiser.com Conversion Pixel
1P Cookie	Visitor ID = 1234	GAID ID = 2345 / Zwieback ID = ABCD	GFP Cookie = 3456	GA = 4567
3P Cookie	Biscotti = BCDE / GAIA = 2345	N/A	Biscotti = BCDE / GAIA = 2345	Conversion Cookie
IP	1.2.3.4	1.2.3.4	1.2.3.4	5.6.7.8
UA	Mozilla/5.0 (Linux; Android 10; Pixel 3a) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.96 Mobile Safari/537.36.gzip(gfe)			
Pseudo Cookie	0x123ABC			
JS - Screen Dimensions	390x600			
p0f OS	Linux 2.2.x-3.x			

Google

GOOG-DOJ-AT-00554795

Chrome - End of 2021 / 2022? (Everything 1P + Anti-Covert Tracking)

	youtube.com	google.com	publisher.com	advertiser.com
1P Cookie	Visitor ID	GAIA ID = 2345 / Zwieback ID	GFP Cookie and Trust Tokens	GA
3P Cookie	GAIA ID = 2345 (Same Party)	N/A	3P Cookies Blocked in Chrome	
IP	Encrypted(1.2.3.4 + youtube.com)	Encrypted(1.2.3.4 + google.com)	Encrypted(1.2.3.4 + publisher.com)	No Ip Logged ? (Otherwise, cross-site joins)
UA Client Hints	Chrome 83; Android 10	Chrome 83; 83.0.4103.96	Chrome 83	Chrome 83; Pixel 3a
Pseudo Cookie (using all Client Hints)	0xABC	0xDEF	0x123	0x456
JS - Screen Dimensions	390x600	Privacy Budget Enforcement 400x100	Privacy Budget Enforcement Error Thrown	Privacy Budget Enforcement 100x200
p0f OS		Linux 2.2.x-3.x (Counts towards Privacy Budget of each site)		

Google

KEY TAKEAWAY: Can't track users cross-site (only within same "company")

GOOG-DOJ-AT-00554796

Research we need to explore?

- How can we achieve cross-site based filters (e.g. co-click) with help from Chrome?
  - Chrome's proposed Aggregated Reporting API
  - FLoC IDs?
  - Bloom filters in Chrome with Differential Privacy?
  - Crypto (Secure Multi-party Computation) + Cloud ML?

- Anti-abuse teams want IPs, but Chrome wants us to move away from IPs
  - We're always asked if we can rely less on fingerprinting and more on Trust Tokens

- Can we build defenses only on 1P information with privacy budget enforcement?

- How well will CG (Q3) and Conversion Spam work with Differential Privacy?

- Optimal 1P Trust Token Issuance logic and developing 3rd party issuers (e.g. whiteops tokens)

- How much entropy does AdSpam need w.r.t a privacy budget?

- Effectiveness of Albus and third party IVT detection within Chrome Privacy Sandbox?

Google

GOOG-DOJ-AT-00554797

ePrivacy & Cookieless ads (August 2020)

- TCF (Transparency & Consent): industry framework for communicating user *consent*
    - TCFv2 cut-off date August 15, 2020 and more user controls.
- **ePrivacy Directive**: EU regulation that requires *consent* to use cookie or similar technology on user's device for non-essential purposes
- Serving cookieless ads:

Narnia 3 (O&O)	Display	Conversions
• Zwieback/Visitor ID is a "mixed" use cookie (essential and non-essential) • Proposal: New AdSpam only cookie or encrypted Zwieback/Visitor (Q3 2020)	• Ads related cookies are not essential. • Serve cookieless ads on reservation and app mediation traffic.	• Conversion tracking needs consent. • Project Macaron Code Yellow

- AdSpam implications:
    - Short term: no cookie based defenses on cookieless traffic
    - Longer term:
        - Modifications to Event Attestation / Trust Token to remove public key
        - On-Device & In-Memory Frequency filtering

Google

GOOG-DOJ-AT-00554798

DTX-951 Page 95 of 181

EventAttestation and WebViews (Q4 2020 -> 2021)

Issues with Hybrid apps
- WebViews have their own cookie jars and separate from AAID/IDFA
  - AdSpam developed Biski to address this
- User Privacy and Transparency controls?
- Ambiguous if dealing with an 'App' or 'Browser'

With Anning - App developers to choose if they are more 'App' or a 'Browser':
- If 'App', then WebView can receive EventAttestation
  - Secure AAID + Basic DroidGuard attestation + Confirmed WebView!
- If 'Browser', then (long term) WebView removes 3P cookies and should use Chrome's Privacy Sandbox APIs
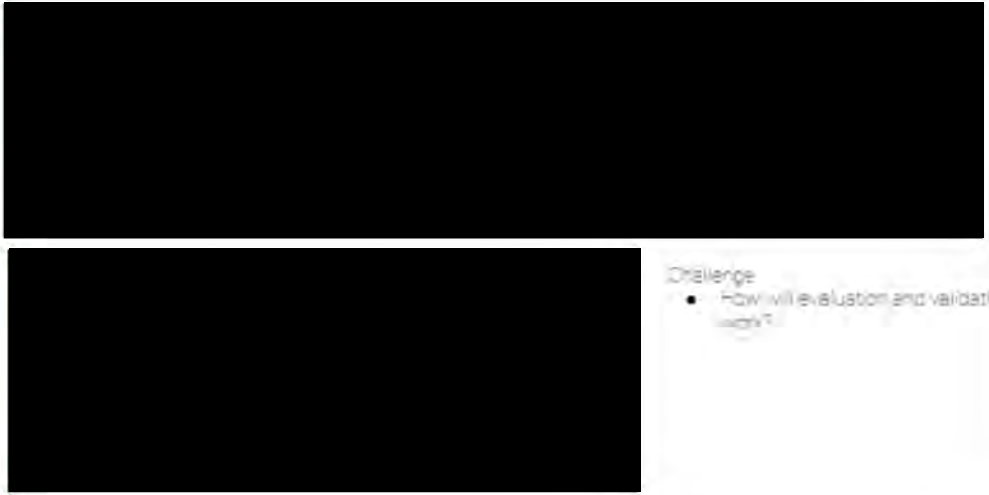
Open questions:
- GDA fragmentation? GDA web and GDA app?
- Is AGSA or Facebook app more 'app' or 'browser'?

GOOG-DOJ-AT-00554799

On-Device Ads (Project Leibniz) and AdSpam

- M1 milestone - AdMob/DRX app inventory, GDA interstitial + DV3 video demand

- Opportunities for *new personalization signals*, but many challenges:
  - No more event level logging (QueryEventMessage, ClickEventMessage)
    - How will past spam, recoveries, credits work in this new paradigm?
    - Pre-bid and post-serve filtration?
  - No more GAIA/AAID/Biscotti ⇒ Cookie Frequency defenses move "on device"
  - Train pModels and combiners on device
  - Graph building (LGP or co-click) on device?
  - New threats:
    - Compromised devices stealing the models or tampering with the weights
    - Access user/publisher/advertiser data
    - Reverse engineer on-device auction

GOOG-DOJ-AT-00554800

On-device Spam Fighting with ML: Options

Challenge
- How will evaluation and validation work?

GOOG-DOJ-AT-00554801

On-device Spam Fighting with ML: Options

"What if we have access to no events server-side, only aggregates?"
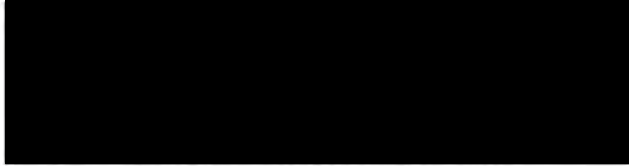
- Per-event prediction and enforcement on-device
- **Several challenges**
  - AdSpam Specific
    - How to build meaningful base model using only aggregated features?
    - How will model monitoring work under differential privacy?
    - Several techniques to "fine-tune". Which technique? How to validate without access to data?
  - General
    - How to prevent stealing and reverse engineering of model and enforcement mechanisms
    - Unclear serving feasibility at AdSpam scale
    - On-device model size, complexity constrained by memory and battery budget

GOOG-DOJ-AT-00554802

Fragmentation of Defenses

- Chrome and other Browsers
  - Will other Browsers adopt Chrome's Privacy Sandbox?

- Chrome Android potentially having more signals through GMSCore
  - e.g. Android Trust Tokens: perhaps on-device integration?

- Browsers vs WebViews
  - Display/Video ads in Browsers (no 3P cookie) vs in WebViews (Injected Event Attestation)

- Conversions
  - non-Chrome Conversions vs Chrome Conversions using Differential Privacy

- Browsers (limited entities) vs Apps (AAID/IDFA and IPs)

- ASML and Android GMSCore on-device

Necessary "remedies", but leads to more complexity?

GOOG-DOJ-AT-00554803

DTX-951 Page 100 of 181

Call To Action

Privacy changes affecting AdSpam are starting **now**!

Be mindful of privacy changes that's coming within ~2 years vs longer term efforts (e.g. on device).

Do we continue to launch web-based defenses using entities/signals that we know are going away within 2 years (e.g., 3rd party cookies, detailed UA and IP, other high-entropy signals)?

Request teams start investing time in new web-based defenses using alternative signals and approaches.

Note: Privacy Team has limited resources with ~3 SWEs and 1 T&S

GOOG-DOJ-AT-00554804

18-month Planning [for Chrome Non-WebView]

	2020		2021				
	Q3	Q4	Q1	Q2	Q3	Q4	
Loss of 3P Cookies	Trust-Token Education/Familiarization		Plan and execute migration off Biscotti-based Signals				**No More 3P Cookies**
			Design and implement new CG based on conversion APIs				
			Design and launch Trust-Token based defenses				
				Assess signals from other Token issuers (Facebook, Amazon, etc)			
			Add infrastructure support for TT-based entities				
Chrome Anti-Covert Tracking		Migrate to UA CH	*Freeze of Full Chrome UAs, eventually will lose this to Privacy Budget*				**Privacy Budget Enforced**
			Adapt to Willful IP Blindness				
			Design and implement Privacy Budget compliant defense approach(es)				

Google

GOOG-DOJ-AT-00554805

Reminder

We (as Google) cannot violate the
intentions of these privacy initiatives
(even if technically possible)

Google

GOOG-DOJ-AT-00554806

Day 2

Agenda

Day 2: Deep dives into key challenges

Keynote by Saikat
High level strategy overview.
break
Trust Graph powered analysis
break
Challenges with supporting new/emerging markets/ segments/ products
Improving precision and monitoring
break
Impression Spam
Apps & Play
Closing Remarks
Fun event

See detailed agenda at go/adscam-strategysummit20-agenda

Google

GOOG-DOJ-AT-00554808

Keynote by Saikat

PST: 7:30am – 7:45am
GMT: 3:30pm – 3:45pm
IST: 8:00pm – 8:15pm

GOOG-DOJ-AT-00554809

Logistics Reminder

❖ Please stick to the allocated time

❖ Allow time for Q&A

❖ Add notes, AI's and follow ups/additional items to the notes doc (go/adspam-strategysummit20-notes)

Misha - 40 sec

GOOG-DOJ-AT-00554810

GOOG-DOJ-AT-00554811

Id	Date	Text
1	06/24/2020 04:49:32	+andresf@google.com +subir@google.com +aruna@google.com Added the strategy slides -- will check early Wed morning if you have suggestions for improvements.

GOOG-DOJ-AT-00554812

Session goals

- Update on progress towards updating the overall AdSpam strategy
- Next steps (call to action)

Google

GOOG-DOJ-AT-00554813

AdSpam strategy doc [work in progress]

go/adspam-strategy-doc

Google

New platform/infra allows us to take it to the next level - what innovations can we build on top of our infra?
We are developing new and promising approaches - clustering, risk modeling, organic labeling, etc.
We are getting much better at leveraging data across Google
Industry collaboration, standards, and hardening the ecosystem is gaining momentum
I think we are ready for take-off to new levels of IVT defenses.

GOOG-DOJ-AT-00554814

Structure of the strategy doc

- Introduction: Summary, background, definitions
- Goals
    - Brief description
    - Key challenges
    - Gaps/risks and opportunities
- Strategic intents
    - Core projects & roadmap
- Major dependencies and risks

Google

GOOG-DOJ-AT-00554815

High level goals

1   Close gaps in IVT defenses and address largest IVT risks

2   Ensuring long-term sustainable IVT capabilities: Build for the future

3   Support safe growth of new ads business

4   Protect Google by increasing IVT defenses and trust across the industry

(Note: these may also be referred to as pillars, focus areas, themes, etc.)
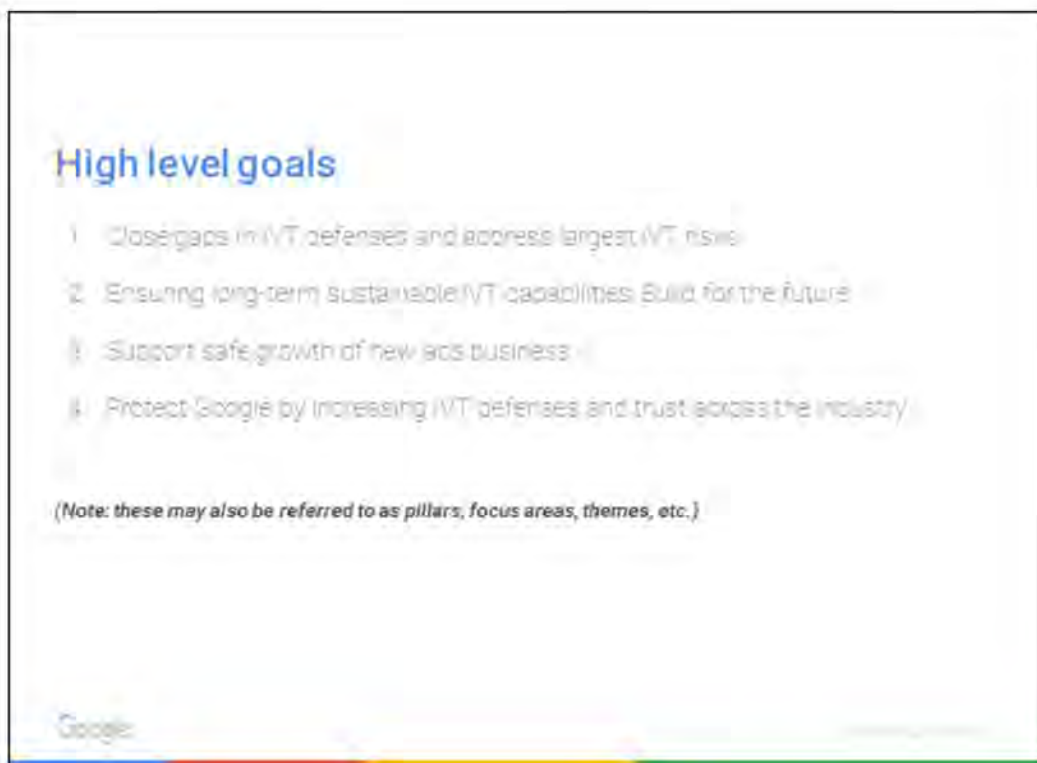
Google

1) Close gaps in IVT defenses and address largest IVT risks
Minimize IVT risk by addressing areas with weak defenses across Google's ads products, and address the largest IVT risks.
2) Ensuring long-term sustainable IVT capabilities: Build for the future
Ensure that AdSpam is able to effectively protect Google's ads business in the future: win the arms race with bad actors, adapt to ongoing shifts in privacy approaches and other ecosystem changes, and evolve in tandem with Google's ads products.
3) Support safe growth of new ads business
Support the sustainable growth of new business opportunities like new ad products, new formats, new environments, new deals, etc. across all of Google's ad product portfolio.
4) Protect Google by increasing IVT defenses and trust across the industry
In order to effectively fight and prevent IVT and ad fraud within Google, we need to increase IVT defenses and trust across the industry at large to minimize overall systemic risk.

GOOG-DOJ-AT-00554816

1) Close gaps in IVT defenses and address largest IVT risks

Description: Minimize IVT risk by addressing areas with weak defenses across Google's ads products, and address the largest IVT risks.

Challenges:
- Large number of surfaces to defend (products, formats, devices, event types, logs, etc.)
- Adversarial nature means we can't launch in a "set it and forget it" mode
- Sophisticated fraud is attractive for some companies and cyber criminals
  - They are highly skilled and can mount sophisticated and scalable IVT operations (attacks)

Google

GOOG-DOJ-AT-00554817

2) Ensure long-term sustainable IVT capabilities: Build for the future

Description: Ensure that AdSpam is able to effectively protect Google's ads business in the future: win the arms race with bad actors, adapt to ongoing shifts in privacy approaches and other ecosystem changes, and evolve in tandem with Google's ads products.

Challenges: Developing a deeper understanding, more comprehensive knowledge, and better methods, tools, and techniques to
- scale with Google's evolving ads products
- adapt to dynamic and increasingly sophisticated bad actors
- maintain defenses in the new privacy-first online environment.

Google

GOOG-DOJ-AT-00554818

3) Support safe growth of new ads business

Description: Support the sustainable growth of new business opportunities like new ad products, new formats, new environments, new deals, etc. across all of Google's ad product portfolio.

Challenges:
- Providing IVT defenses for new products and deals that may not "fit the mold"
  - new interaction models
  - not using "standard" ads backends (e.g., logs)
- Supporting custom deals while maintaining economy of scale and avoiding one-off solutions
- Achieving defensibility in environments that lack signal collection

Google

GOOG-DOJ-AT-00554819

4) Protect Google by increasing IVT defenses and trust across the industry

Description: In order to effectively fight and prevent IVT and ad fraud within Google, we need to increase IVT defenses and trust across the industry at large to minimize overall systemic risk.

Challenges:
- Sharing information without
  - leaking privacy sensitive data
  - giving the secrets to "bad guys"
- Hard to motivate an industry mostly focused on short-term revenue to invest for the long-term sustainability
- Lack of ground truth/effective advertising ROI metrics makes it hard to justify investments
- Monetary incentives not always aligned with sustained and effective IVT defenses

Google

GOOG-DOJ-AT-00554820

Topics to consider for L2 strategic intents

Some ideas/food for thought:

- Not relying on 3rd party cookies for AdSpam defenses
- "Connect the dots" leveraging data from across Google (Trust Graph etc)
- Impression defenses on par with click defenses
- Know your users and partners (entities, pubs, supply partners, sites, apps, etc.)
- SIVT level defenses for all DCLK products
- Productivity/time from attack to launch
- Use organic labeling across all areas
- 95% of all IVT from cases covered by major press outlets have been filtered by Google

Google

GOOG-DOJ-AT-00554821

Next steps

- Overall AdSpam
  - Review and provide feedback on top level strategy doc (what's missing?) *(due Aug 14)*
  - Brainstorm and align on L2 strategic intents *(draft due July 10; final due Aug 14)*
  - Who: PMs, TLM/TLs, PgMs, T&S leads

- Team-level *(due Aug 14)*
  - Develop team strategy
  - Define team level strategic intents
  - Outline projects/roadmaps to achieve strategic intents

Google

GOOG-DOJ-AT-00554822

GOOG-DOJ-AT-00554823

GOOG-DOJ-AT-00554824

Building for the next generation of AdSpam impact

- Thesis: as our ads products continue to grow in size and complexity, and as bad actors continue to innovate, the key to our success will be our ability to scale

- There are many components to scaling (including automation), but we will always be dependent on human insights to understand the problem space

- Building tools that enable our analysts and engineers to achieve maximal impact will be a critical part of AdSpam's success

- TrustGraph, and apps using TG data (eg. TG Insights, Telescope, and SmartLeads), will be key drivers of innovation in detection and our ability to scale

Speaker: Zack

a) educate (feedback I keep hearing is folks dont know the vision/plan)
b) build enthusiasm (some selling on the future potential - but not overselling)
c) feedback / alignment

GOOG-DOJ-AT-00554825

Speaker: Zack

GOOG-DOJ-AT-00554826

TrustGraph Feature Offerings

- **Assess: look up, explore, & build holistic xPA assessments**
  - Enhance understanding of the world by better leveraging cross-PA anti-abuse data

- **Contribute: enable users to painlessly bring data to TG**
  - Encourage and empower users to bring data to TrustGraph

- **Mine: enable teams to extract max value from their data using TG**
  - Find abuse at scale, and automatically generate insights about your data

- **Act: enable teams to take anti-abuse actions using TG**
  - Enable users to take action via their preferred channels

Google

Speaker: Zack

GOOG-DOJ-AT-00554827

Talking points:
analysts can browse data using a combination of graphs and tables
mention that we have graph extraction (aka graph query language 0.5) as input
first version of this will be Smartmeter
would like to get feedback on the possibility of integrating this with other investigation tools

GOOG-DOJ-AT-00554828

Id	Date	Text
1	06/22/2020 21:14:25	@xinzhao@google.com Please take a look at this slide and the next one. I plan to verbally say that these 2 UI would be combined at some point in the future in Smartmeter. Does this sound good to you? @zacharylf@google.com for a FYI _Reassigned to Xin Zhao_
1	06/22/2020 21:14:25	SG. This is indeed our plan. The graph help visualize the most relevant clusters/nodes, while tables provide detailed info and highlights from users' interpretation on signals.

GOOG-DOJ-AT-00554829

Assess via a Table

GOOG-DOJ-AT-00554830

Browsing Metadata
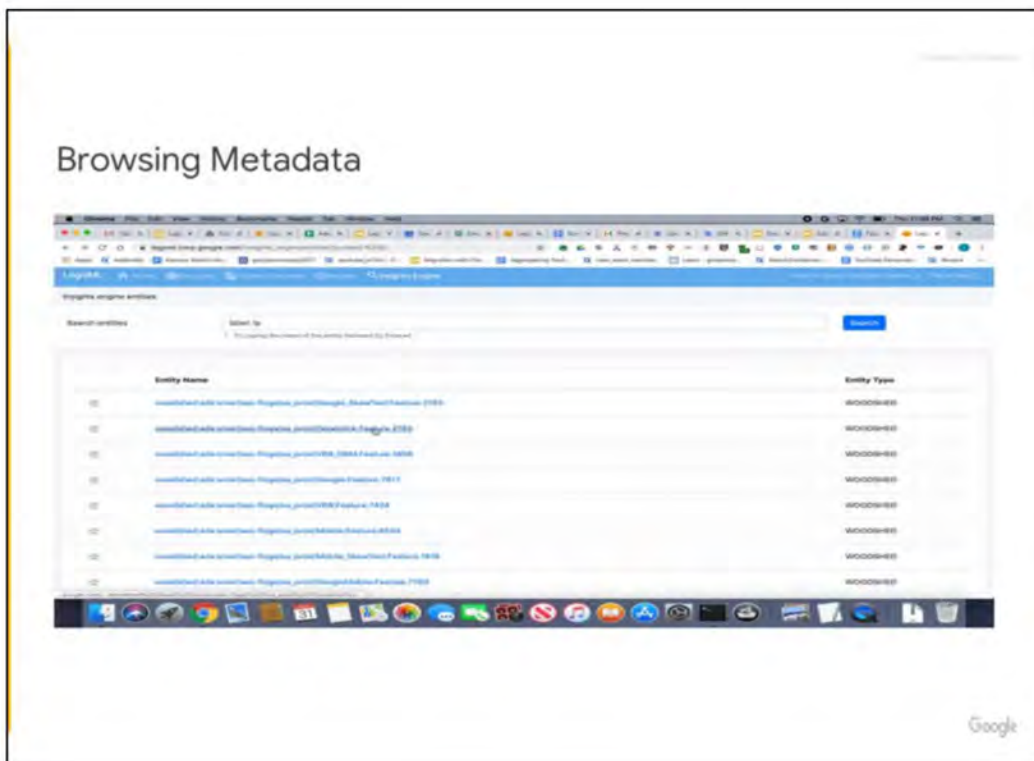
Might skip this if we don't have time

Mine: What TrustGraph brings to Adspam
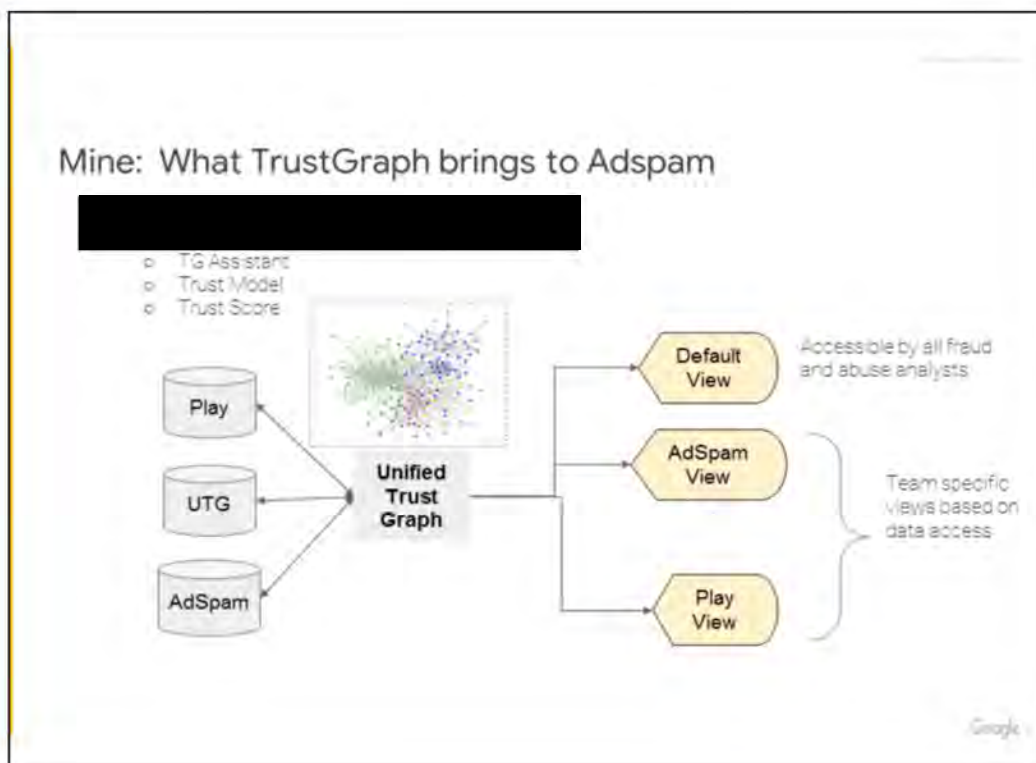
Unified Trust Graph -> Trust Model -> Trust Score

Recent Wins: (Q1/Q2)

- **Within Adspam:**
  - ○ [Q2] User Trust Graph ($35M ARR)
  - ○ [Q2] Mobile Model Disruptive Ads v3 ($8.1M ARR)
  - ○ [Q2] AdspamRisk - AdMob Unified Model ($100M ARR)
  - ○ [Q1] AdspamRisk - Online Graph Mining ($11M ARR)
  - ○ [Q1] AdspamRisk - Admob Risk Propagation Model ($12M ARR)

- **Outside of Adspam:**
  - ○ [Q1] AI^2 - Offline Graph Mining for UBP ($40M ARR)
  - ○ [Q1] Android App Security Eng - 12k developers caught annually
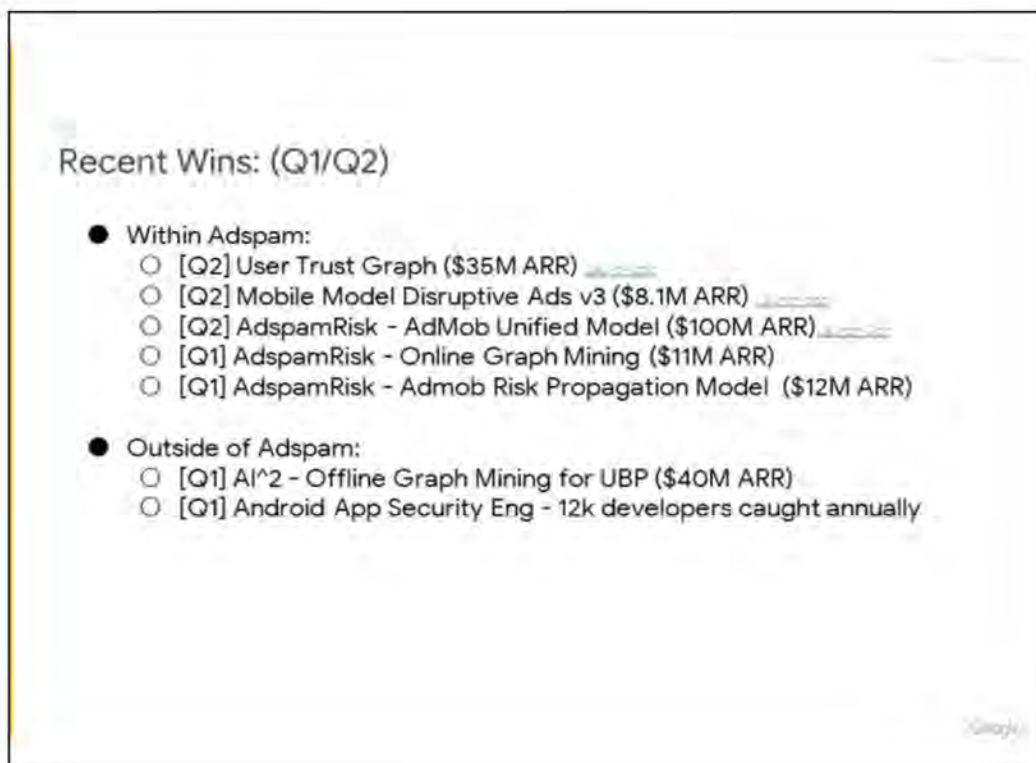
There are some launches here that we could include.

GOOG-DOJ-AT-00554833

Id	Date	Text
2	06/22/2020 18:10:38	@kalpa@google.com
3	06/22/2020 21:17:47	Just added ones from here: https://docs.google.com/document/d/1AN7Ht8j6rwtGVUYwZe0la2HI8fCbsSzF20NWHdcqs2Y/edit#
1	06/22/2020 21:26:21	I am unable to edit but we should add these launches too - https://docs.google.com/presentation/d/1z7iyGGJEL8Kf9Rb1Ily7VwTbgUH1OH568SlwM0z6BTc/edit#slide=id.g7e4601850f_1_0
1	06/22/2020 23:34:41	+hsiaosu@google.com Do you have any material on early wins for UTG and AdSpam Risk we can highlight here?
4	06/22/2020 23:34:41	I filled out a few more from here: go/tg-impact&engagement-tracker

GOOG-DOJ-AT-00554834

Simplify this slide, stress that we'll make privacy easier.
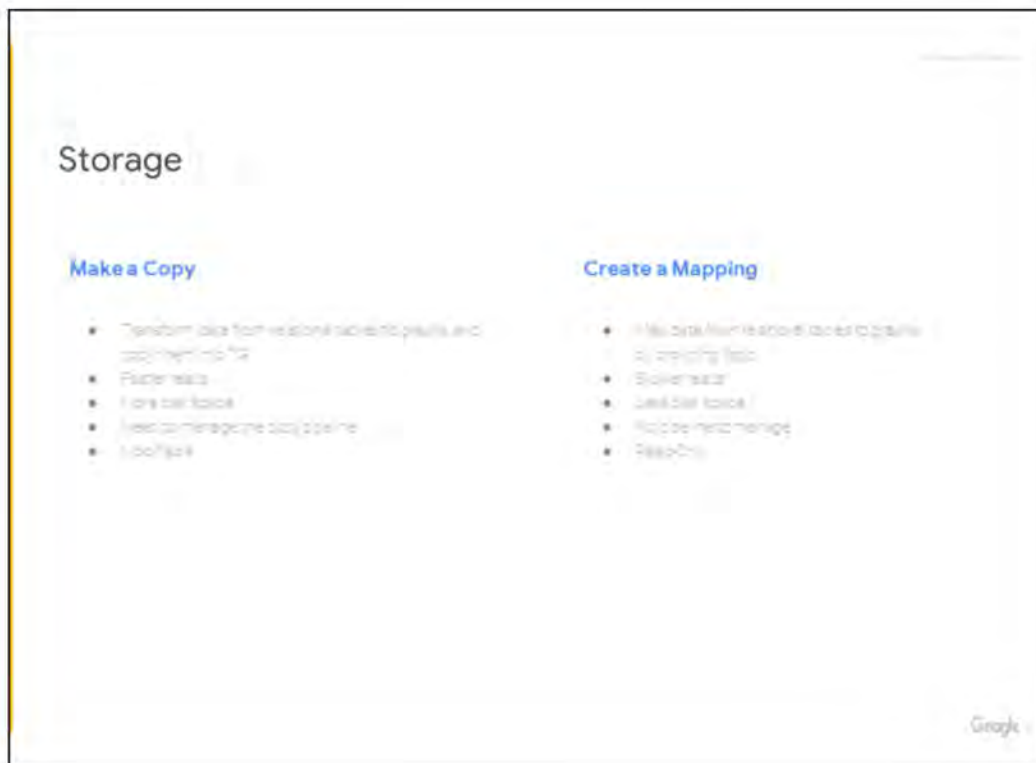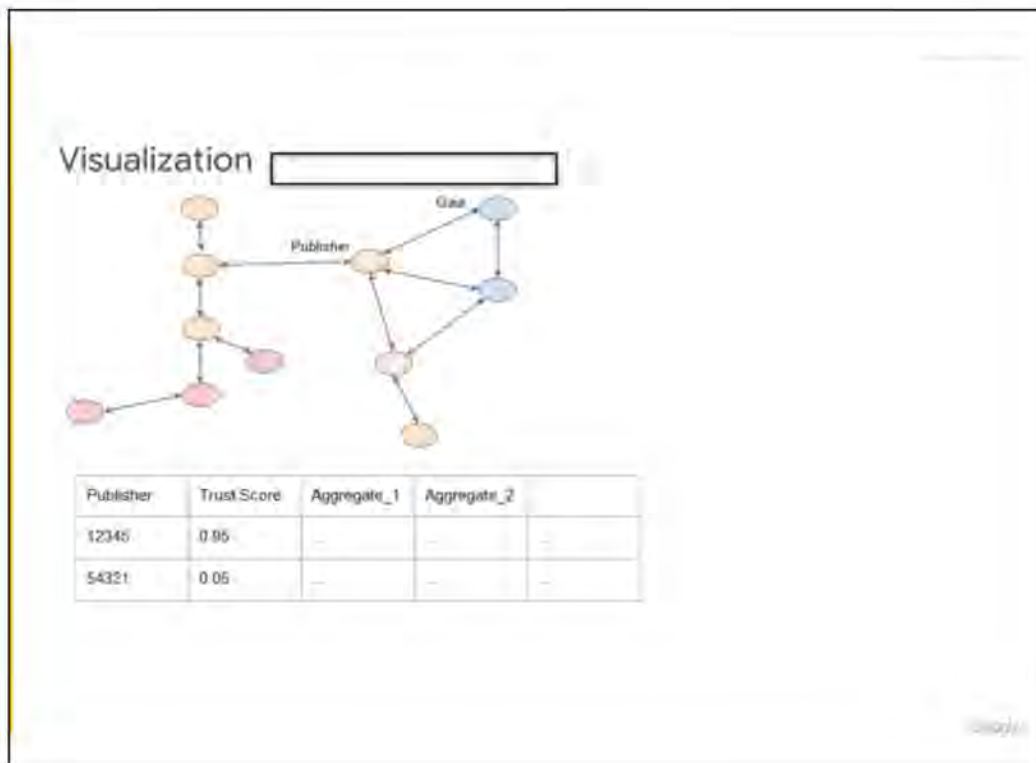
GOOG-DOJ-AT-00554835

Skip this

GOOG-DOJ-AT-00554836

Talking points:
analysts can browse data using a combination of graphs and tables
mention that we have graph extraction (aka graph query language 0.5) as input
first version of this will be Smartmeter
would like to get feedback on the possibility of integrating this with other investigation
tools

DTX-951 Page 135 of 181

GOOG-DOJ-AT-00554838

GOOG-DOJ-AT-00554839

Goals

- Review some of the key trends and challenges driving complexity in our space
- Start a discussion around how we should address those challenges as an organization in our 2021 strategy planning

The goal of this session is to seed a conversation about the big picture trends and challenges facing AdSpam as we go about our 2021 planning.

This isn't a TED talk, I don't have a crystal ball, but hopefully this will start a useful discussion and help us frame our annual strategies in a way to address some of these challenges.

GOOG-DOJ-AT-00554840

AdSpam operates in a complex and dynamic space

- The Digital Ads Ecosystem is constantly growing and evolving
- Google is itself a large, complex organization with a wide array of products both new and established needing AdSpam support.
- AdSpam has been relatively successful in standardizing our policies and requirements to enable us to scale across Google's ads business and integrate most new products.
- However, there are an increasing number of new products and requests that don't fit neatly into our standardized solution, requiring custom work and constant realignment.

The main drivers of complexity appear to be accelerating. What else can we do to get ahead of the problem?

AdSpam operates in a really complex space. Externally, the digital ads ecosystem is growing, evolving, and maturing - reaching new forms of media.

Internally, Google's variety of businesses, infrastructure, and organizational structure is extremely complex in its own right.

We've developed ways to help us navigate complexity (like alignment), and address it more structurally through standardizing our integration requirements, and innovating in our analysis methodologies and infrastructure (eg, ASML, TrustGraph, Organic Labeling).

This has helped us be relatively successful in both supporting new product requirements and feature requests, and scaling our defenses across Google's wide array of businesses, as part of our "standard solution"

The emerging trends that are driving the complexity we deal with on a daily basis, originating both internally and externally to Google, are pointing to an expansion in variety and diversity of online ad experiences for users and platforms where they happen.

As a result, we're increasingly seeing requests fall outside of these standard processes and solutions, requiring custom work and constant alignment.

GOOG-DOJ-AT-00554841

As we go through strategic planning, how can we get ahead of these trends? Are there any asymmetric bets we can invest in in 2021?

Starting with external trends:

The ads ecosystem follows user behavior. Increasingly, users are engaging with ad supported content across a higher number and wider variety of devices. We've all heard about the shift from desktop to mobile, and now we're seeing the beginnings of a shift to wearables, smart speakers, and connected TV devices. New devices, ad formats, attack vectors, signals and collection mechanisms, all require additional attention from AdSpam.

The second trend to call out here is similar - as the digital ads ecosystem matures, we're starting to see a shift in "traditional" ad spend moving to digital, and from digital to programmatic. While CTV, DOOH, and Audio are all multi-billion-dollar markets already, look at how much is still spent on their traditional siblings -- over $250B!

Not all of this will move to digital, and what does isn't going to move all at once, but I think this does at least hint that we'll continue to see continued growth in these new areas for the years to come.
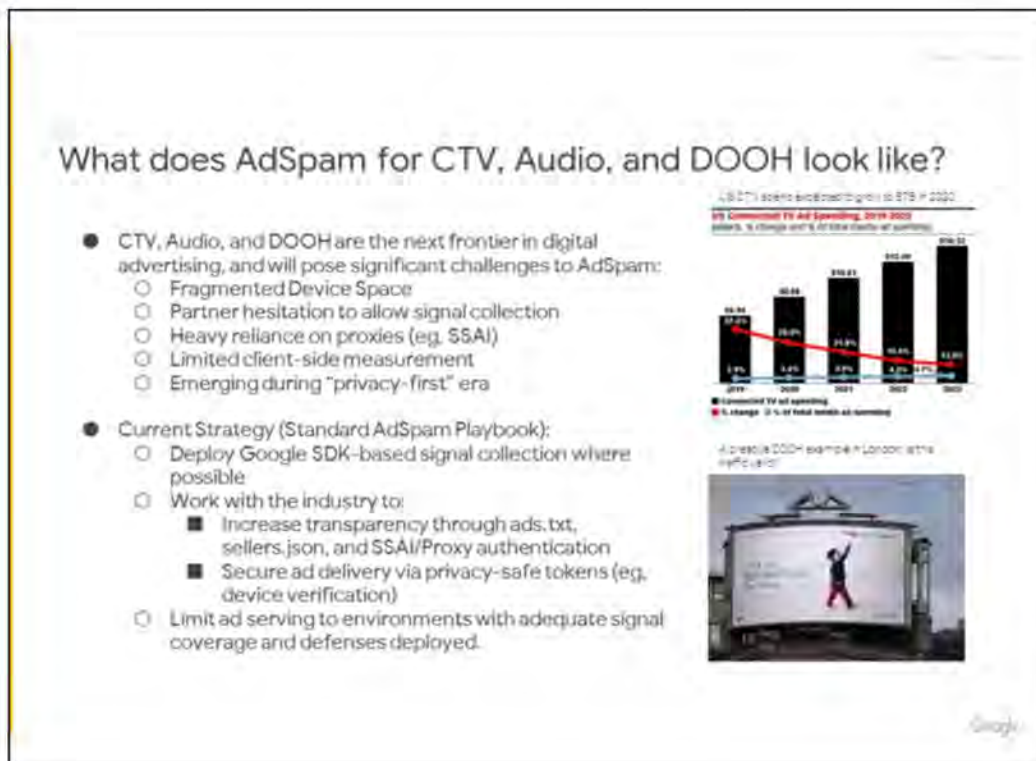
GOOG-DOJ-AT-00554843
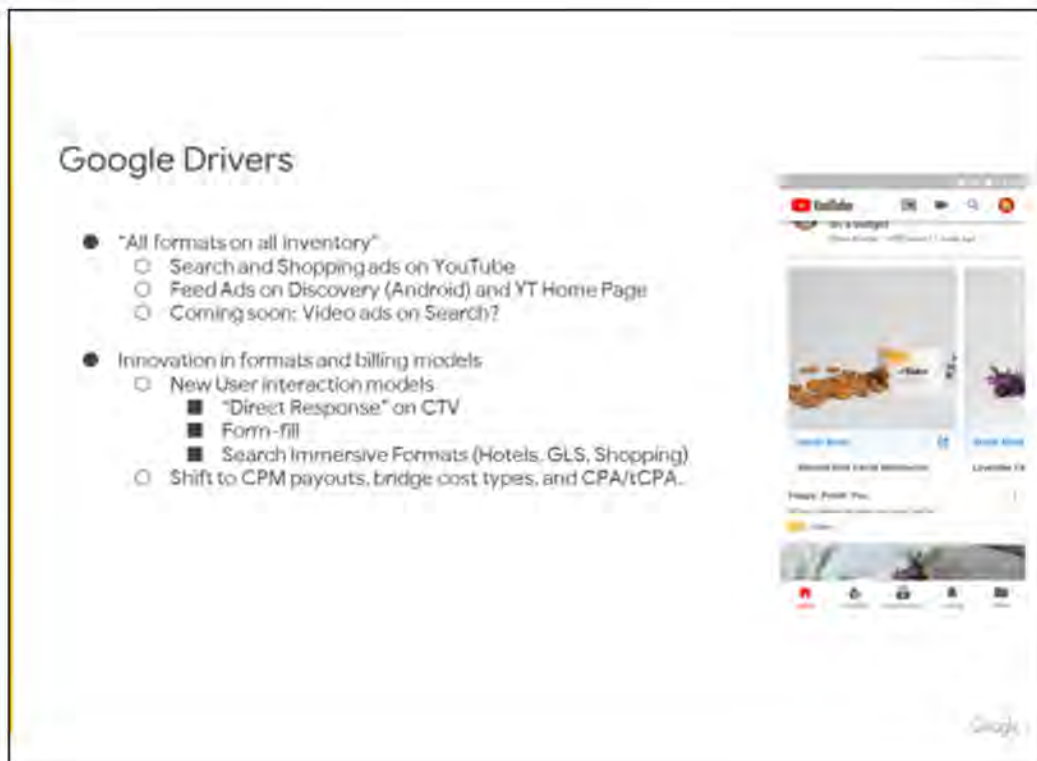
Within Google, we're increasingly seeing an effort to consolidate ad format and inventory offerings, to allow advertisers to run the same ad in more places. For example, if you look at recent developments in the YouTube app, you'll notice AFS ads, Shopping ads, and Feed ads have been incorporated into the Home and Search pages.

At the same, innovation in formats and billing models are challenging some of AdSpam's assumptions around expected user interactions, metrics, and even logs and event-hierarchies.

For example, in immersive formats on Search such as Shopping, Local Services, or Maps, we often log multiple clicks for each ad - the first is to open the immersive, the second is the ad click. Enhanced Conversions have found that their requirements can't be met with the AdEvents logs.

GOOG-DOJ-AT-00554844

What does AdSpam for CTV, Audio, and DOOH look like?

- CTV, Audio, and DOOH are the next frontier in digital advertising, and will pose significant challenges to AdSpam:
  - Fragmented Device Space
  - Partner hesitation to allow signal collection
  - Heavy reliance on proxies (eg. SSAI)
  - Limited client-side measurement
  - Emerging during "privacy-first" era

- Current Strategy (Standard AdSpam Playbook):
  - Deploy Google SDK-based signal collection where possible
  - Work with the industry to:
    - Increase transparency through ads.txt, sellers.json, and SSAI/Proxy authentication
    - Secure ad delivery via privacy-safe tokens (eg. device verification)
  - Limit ad serving to environments with adequate signal coverage and defenses deployed.

By way of example: CTV, Audio, and DOOH are the "next big thing", and incorporate a lot of these trends.
[DEFINE THE TERMS]

We're the furthest along in our defense of CTV, and so far, we've tried to apply the standard AdSpam playbook.

As we expand down the long-tail of CTV devices, and into smart speakers and billboards, do we need a different approach? How does the definition of IVT change for these formats?

Recent shifts if Mobile app advertising and related abuse vectors are also rapidly changing, and challenging us in unique ways - I believe Zack is going to cover some of these in a future session.

GOOG-DOJ-AT-00554845

Key Takeaway: New Business Requirements

Based on these trends, and the direction of the digital ads ecosystem more generally, there are two primary new requirements:

1. Increased diversity in user interaction models
2. Increased diversity in technical implementations

So how do these trends affect AdSpam?

These trends are pointing to two new business requirements that we'll need to find a way to support.

GOOG-DOJ-AT-00554846

AdSpam Challenges

These new requirements will pose some significant challenges for AdSpam:

● **Signal Collection:** As the number and variety of device platforms and implementations needed to support the ads business expands, it will be difficult to ensure adequate and consistent signal collection.

● **Non-Standard Implementations:** As more products require custom work from AdSpam, it will increasingly be a challenge to scale and maintain our defenses across all of Google's businesses.

● **Organizational Alignment:** As formats, signal collection mechanisms, and device platforms shift, does our organizational structure and vertical/horizontal team structure set us up for success?

● **Elevated Operational Costs:** Any gaps or shortcomings in our approach to defending new products increases the operational burden on our T&S teams.

Google

And becoming flexible enough to support those new requirements won't be easy.

GOOG-DOJ-AT-00554847

DTX-951 Page 144 of 181

Key Questions for Strategic Planning

- How do we build for flexibility, while still supporting new products?
- How do we maintain defense quality in signal-poor environments?
- How do we impact product roadmaps, and/or decide which products to support?
- What is the right balance to strike between defending a product area where it is, vs. requiring it to change before we can offer support?
- Can we come up with a new engagement model that enables us to scalably support more of the requests currently considered "custom"?
- Are there any asymmetric bets we can invest in today to help us prepare to meet these challenges?

So as we go through this strategic planning summit and related exercises, I think there are a few key questions that I hope we can keep in the back of our minds.

GOOG-DOJ-AT-00554848

GOOG-DOJ-AT-00554849
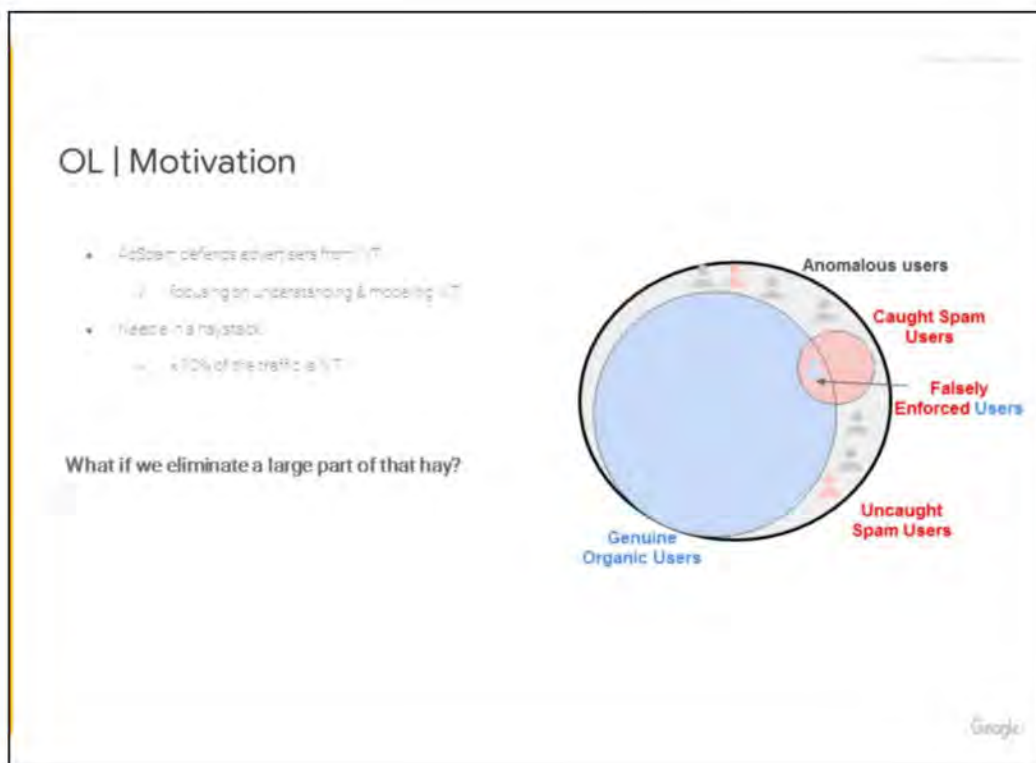
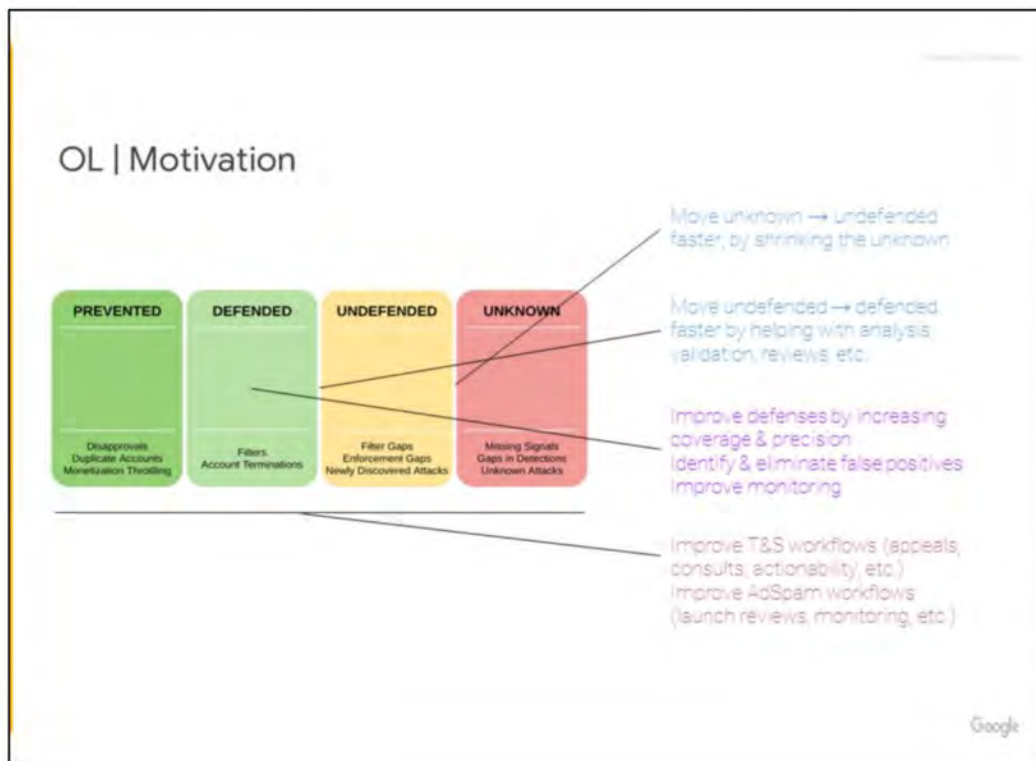| Id	Date	Text	
1	06/16/2020 22:03:35	@spacemanspiff@google.com @atali@google.com	Proprietary + Confidential
1	06/16/2020 22:03:35	@sulabha@google.com I think you had a couple slides to share too	

GOOG-DOJ-AT-00554850

Organic Labeling (OL)

Organic Labeler is one that labels entities having no evidence of spam
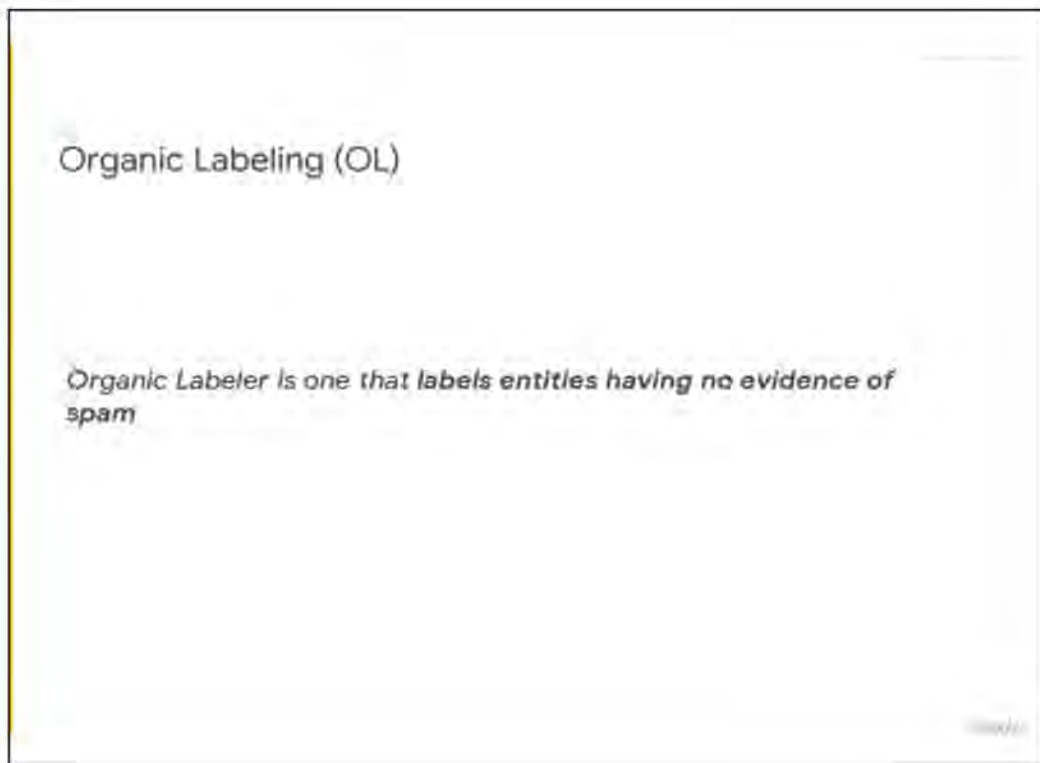
Slides heavily stolen from a bunch of different slide decks by rahulmah@.
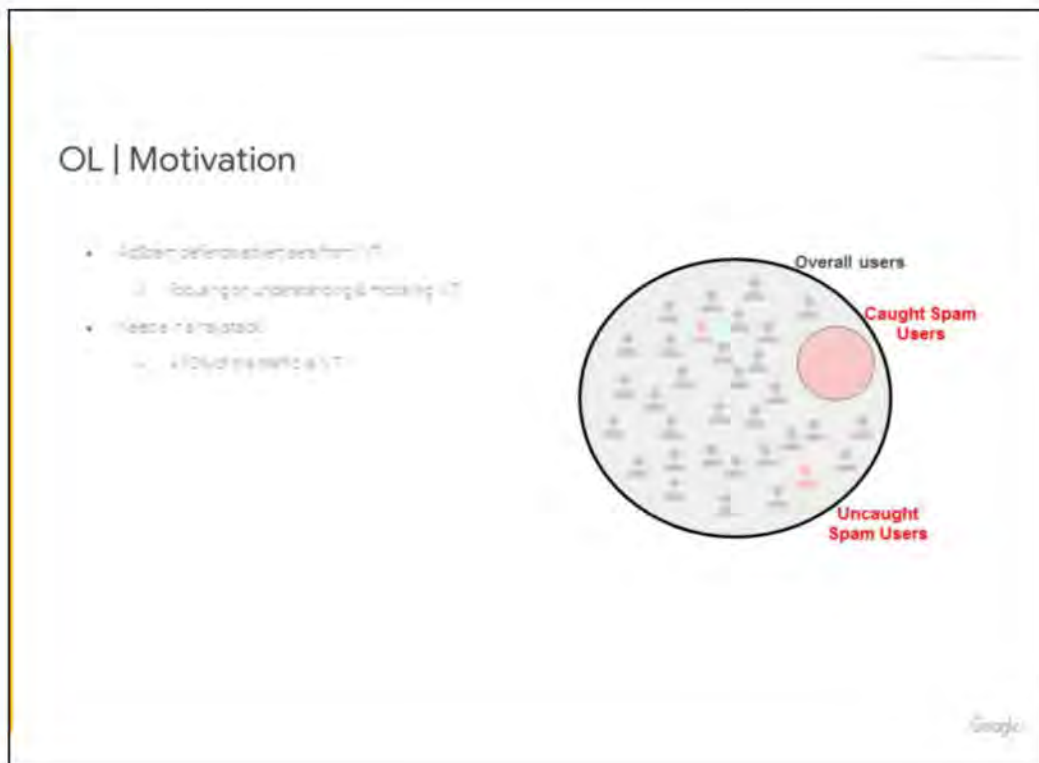
GOOG-DOJ-AT-00554851

Uncaught spam << 0.5%.

GOOG-DOJ-AT-00554852

Uncaught spam << 0.5%.

GOOG-DOJ-AT-00554853

GOOG-DOJ-AT-00554854

GOOG-DOJ-AT-00554856

DTX-951 Page 153 of 181
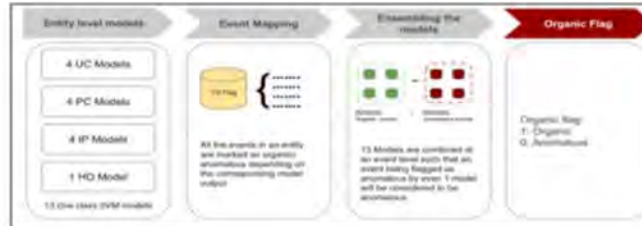
rahulmah: As per OL insights we know that at least 30-40% FPs are in form of collateral damage and turn downs are not the complete solution? We expect this to be the case across verticals as well.

GOOG-DOJ-AT-00554857

OL | There's more

- Identification of anomalous existing organic traffic (SHOCT, TTS, gTSF etc.)
  - Starting up automated escalations
- Improve DrySar's performance
- Optimization of many T&S processes (eg. Arbitration by actionability)
- Insights into which pockets of traffic we need to focus on
- Monitoring ASOR, UOR
- Streamlining manual reviews & launch reviews
- Integration with User Trust Graph

GOOG-DOJ-AT-00554858

GOOG-DOJ-AT-00554859

Impression Spam - Problem Statement

Ad impressions are much less well-defended across Google's ad products than are ad clicks...

...yet impressions represent > 50% of total monetized ad spend.

As of early 2020, the dollar-weighted pure CPM-based IVT rate is 1.6%, vs CPC-based IVT rate of 8.1%

Meanwhile, publishers already have, and face new incentives, to inflate impressions:
Impressions are already the event by which GAM publishers are paid for monetization, and will be for AdMob in 2020, and AdSense in 2021.

Google

Speaker: Zack

GOOG-DOJ-AT-00554862

Impression Spam - But How Big?

Extra Sensitive!

We estimate:

Upto $300M ARR uncaught IVT on pure CPM cost-type

Upto $470M ARR in net loss to Google on the CPC-to-CPM bridge

Supported by multiple,

Independent analyses

Speaker: Zack

GOOG-DOJ-AT-00554863

DTX-951 Page 160 of 181

Impression Spam - Vision and Goals

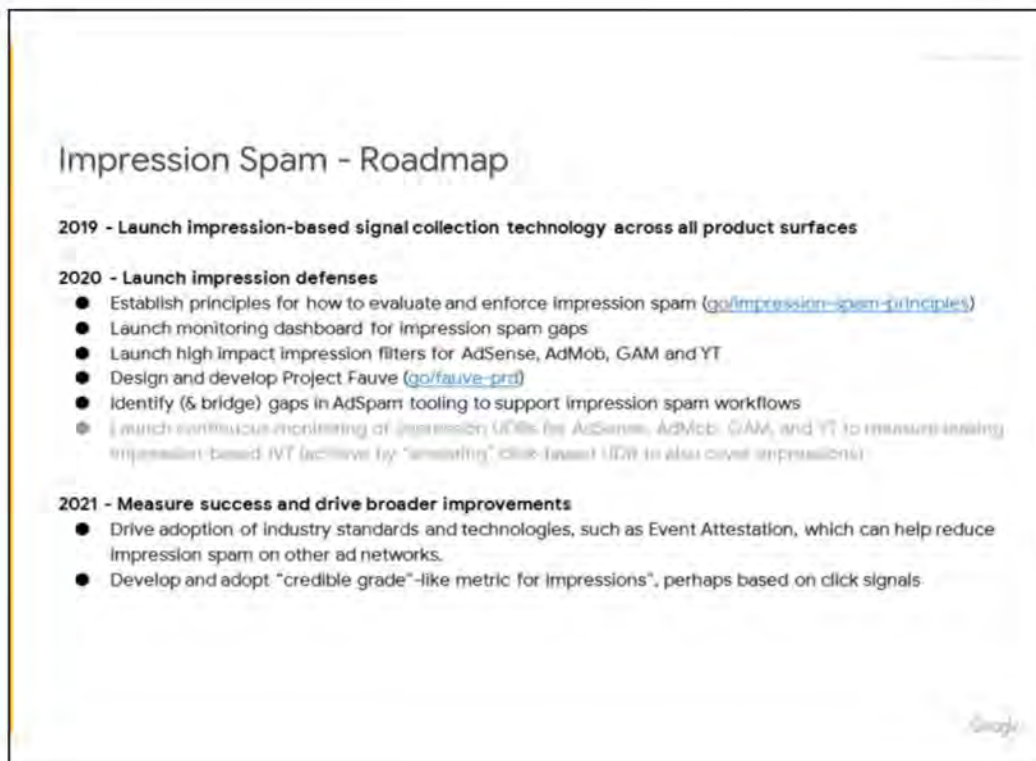**Vision:** *IVT on ad impression is as equally well defended as IVT on ad clicks.*

Goals, in order of priority:

1) We do not charge advertisers for invalid impressions, wasting spend and eroding ROI.

2) We do not pay publishers for invalid impressions, incentivizing more fraud and abuse.

3) We protect both advertisers from underfiltration and publishers from overfiltration.

Google

Speaker: Zack

GOOG-DOJ-AT-00554864

Impression Spam - Roadmap

2019 - Launch impression-based signal collection technology across all product surfaces

2020 - Launch impression defenses
- Establish principles for how to evaluate and enforce impression spam (go/impression-spam-principles)
- Launch monitoring dashboard for impression spam gaps
- Launch high impact impression filters for AdSense, AdMob, GAM and YT
- Design and develop Project Fauve (go/fauve-prd)
- Identify (& bridge) gaps in AdSpam tooling to support impression spam workflows
- Launch continuous monitoring of impression UDFs for AdSense, AdMob, GAM, and YT to measure missing impression-based IVT (achieve by "extending" click-based UDF to also cover impressions)

2021 - Measure success and drive broader improvements
- Drive adoption of industry standards and technologies, such as Event Attestation, which can help reduce impression spam on other ad networks.
- Develop and adopt "credible grade"-like metric for impressions", perhaps based on click signals

Speaker: Arun

GOOG-DOJ-AT-00554865

DTX-951 Page 162 of 181

Impression Spam 2020

- **Formed Impression Spam Working Group** in Eng, and in T&S
- **WhiteOps Integration based augmented defenses**
  - Albus 3PE (Q3)
- **Direct Impression defenses** (aka native defenses)
  - GDA pCookie/pCTR models doubled query spam rate from 1.08% to 2.00% (criteria M 010012)
  - Mobile pCookie/pCTR models (Q3)
  - GVP pCookie/pCTR (H2, maybe)
- **Transfer Learning based Impression defenses**
  - GDA Click to Query impression defenses (Q3)
  - Mobile Click to Query (H2)
- Imputations
- Prevention

Call to Action:
- **Understand** how CPM and CPC-to-CPM impacts and affects your products
- **Help us** improve our measurement of impression spam, and understanding of top attack vectors
- **Drive** impression spam defenses on your networks, leveraging product specific signals, and shrink the gap

Google

Speaker: Arun?

GOOG-DOJ-AT-00554866

DTX-951 Page 163 of 181

Challenges with reviewing Impression Traffic

Metrics Lack of strong validation/re-tuning traffic metrics like CG (like credible grade for clicks)
- Increased review time
- Risk of missing significant clusters of spammy traffic.

Signals Increased dependencies on signals outside of traditional logs (Chrome-ATM, GodCluster)
- Overfiltration risk due to non traffic signals used as spam indicators

Tools Query information split in multiple log sources which slows down investigations

Tools Most of the infra has limited support for Queries.
- e.g., Woodshed has 10% of 1% AEQ data which can be misleading

Tools Tools like Dojo & WPI provide limited support for query or impression level action

Research Limited coverage, understanding & research for existing impression signals

Research Understanding of impression spam not on par with click spam across the team, missing case studies and similar documentation

Google

Speaker: Prachi

GOOG-DOJ-AT-00554867

Impression Spam Principles - A Re-Think

1) **Detecting Invalid Impressions at Scale Requires Using Downstream Events**
   a) TLDR: Can we create an "ImpressionCredibleGrade" to assess baskets of events?

2) **The Law of Spammy Entities - Part 1 - Verdict Transferability**
   a) TLDR: If the clicks associated with a particular entity are spammy, our default position should be to assume the impressions are invalid

3) **The Law of Spammy Entities - Part 2 - Pipeline Transferability**
   a) TLDR: If you determine a particular entity has invalid clicks and impressions on GDA, you should bias towards blacklisting this entity on other demand sources (eg. DV360)

1) **Impression Spam Requires an Appropriate Precision Bar**
   a) TLDR: We should determine an acceptable precision bar for impression spam defenses, which may be lower than for click defenses

go/impression-spam-principles

Google

Speaker: Zack

GOOG-DOJ-AT-00554868

## Impression Spam Solutions – Les Fauves!

- **While we aim to launch impression-event classification, there may be limits**
  - Transfer learning, imputation, entity labeling - all will help significantly
  - Impression metrics will also help
  - BUT there are probably limits that will prevent complete parity with clicks

- **But we can also use auction levers to a) better defend and b) gain information**
  - Eg. Project Fisher prevented conv spam, but not by better marking conversion spam

- **Proposed solution – Project Fauve** (what's in a name anyway?)
  - Develop risk models that identify publishers likely to drive impression spam
  - Apply mechanism to shift demand pre-auction from CPM to CPC
  - Metrics, models, and dashboards to interpret observed changes post-treatment

TLDR: instead of better classifying invalid impression events, lets classify risky publishers, and require them to generate clicks in order to generate revenue

go/fauve-prd

Google

Speaker: Zack

GOOG-DOJ-AT-00554869
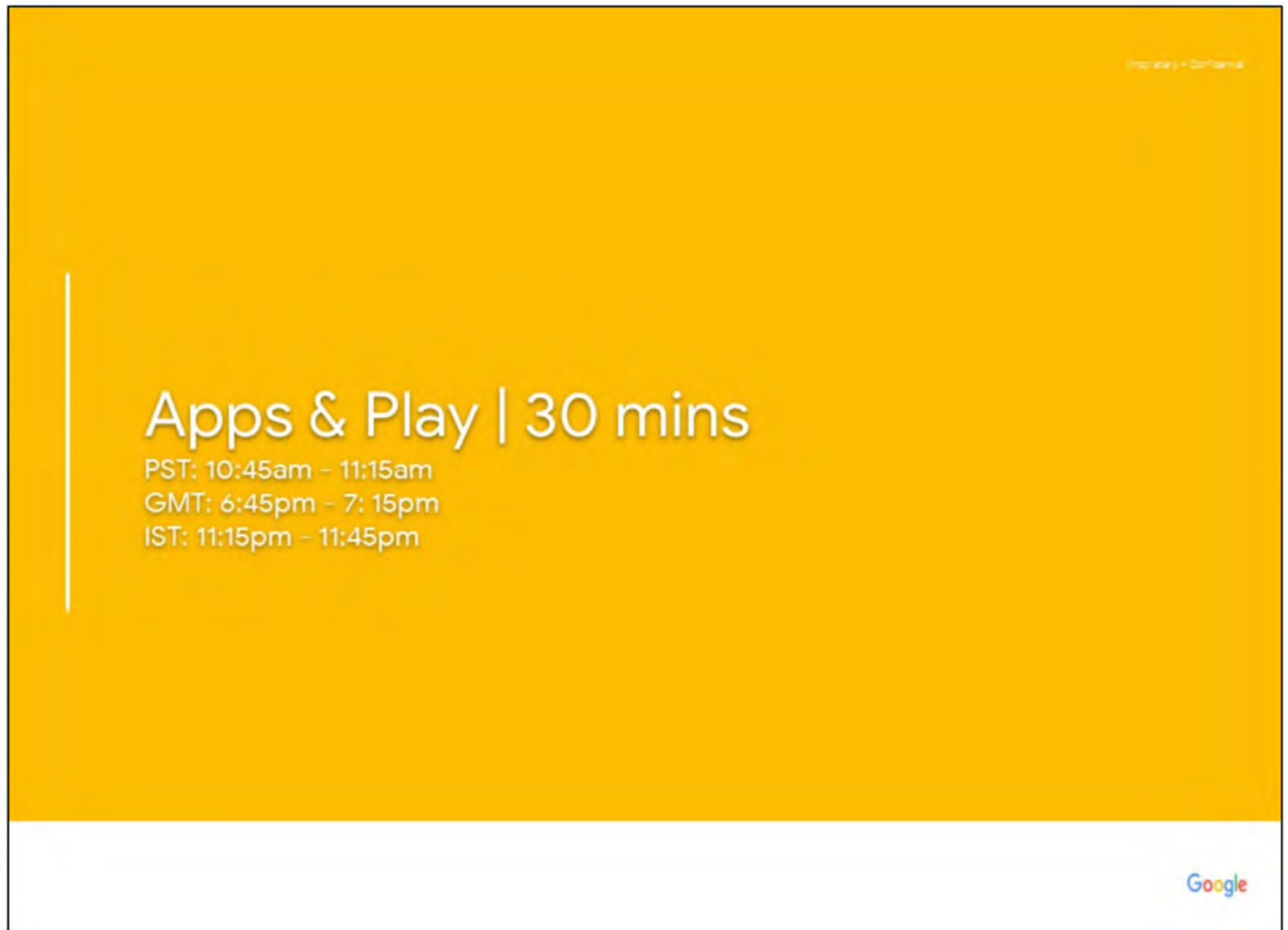
Speaker: Zack

ASE + AdSpam Joint-2020 AdFraud Roadmap

2020 AdSpam+Apps Safety PA-level OKR
Reduce ad fraud on Play by $100M (go/adfraud2020)

1. Reduce latency & expand enforcement
   a. Align enforcement principles and practices across top abuse vectors

2. Programmatic signals, verdicts, & leads sharing
   a. Eliminate organizational information gaps and maximally leverage signals and leads across PAs

3. Improve detection & classification
   a. Dramatically improve both independent and joint ad fraud detection & classification recall

Speaker: Zack

GOOG-DOJ-AT-00554872

2020 Jan 1 State

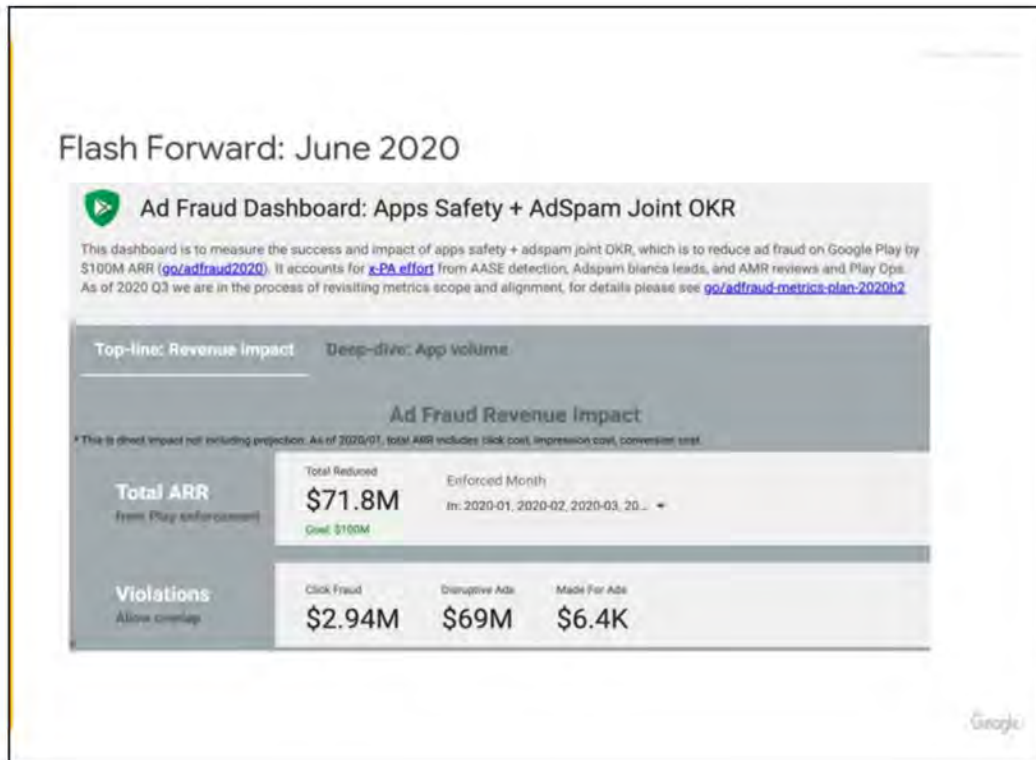|	Reduce latency & expand enforcement	Programmatic signals, verdicts, & leads sharing	Improve detection & classification
Summary	Align enforcement **principles and practices** across top abuse vectors	**Eliminate organizational information gaps and maximally leverage** signals and leads from across PAs	Dramatically **improve both independent and joint** ad fraud **detection & classification** recall
2019 EOY State	**State: weak** Ad-hoc alignment on large enforcement cases. Largely lacking principle and process alignment.	**State: improving** Bi-directional sharing largely offline, via spreadsheet. Some investment with Trust Graph onboarding and leads sharing with SmartLeads.	**State: improving** Historically weak on top abuse vectors. Large launches and momentum building through 2019. On track for large 2020 gains.
Target 2020 EOY State	Aligned on shared principles with enforcement processes deployed across teams	Enforcement status, core abuse signals, risk scores, classification outputs, and prioritized leads from ASE, AdSpam, and T&S universally available in Trust Graph and SmartLeads	Individually and jointly-owned detection and classification techniques launched, providing coverage for > x% of enforced ad fraud on Play

Speaker: Zack
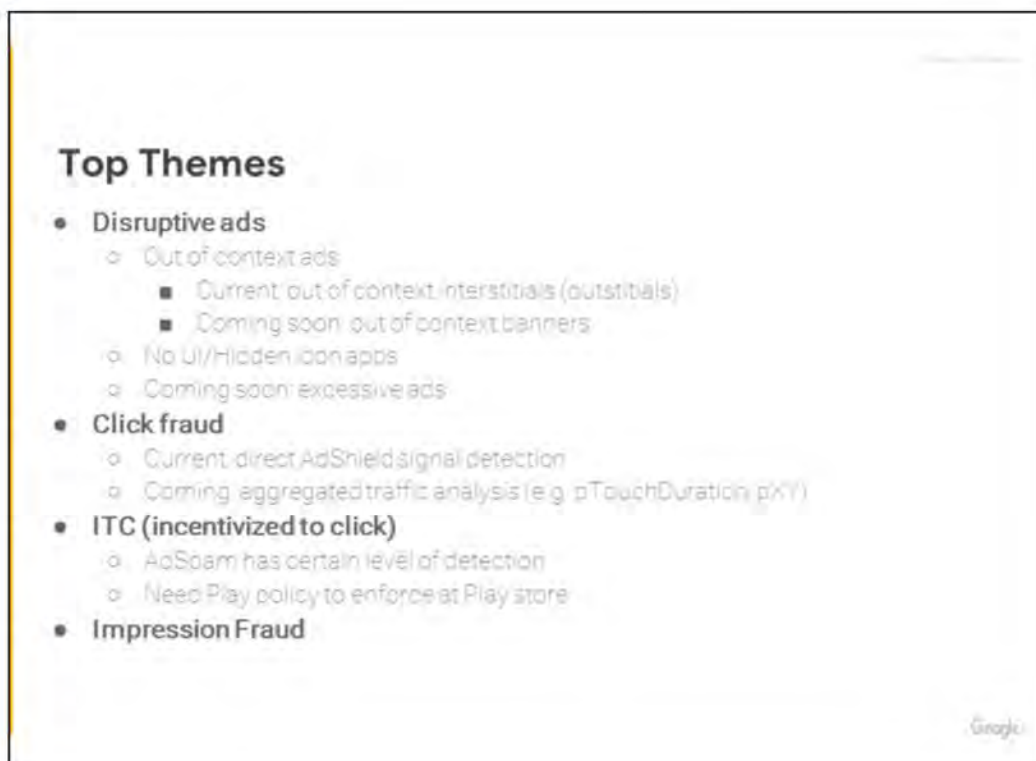
GOOG-DOJ-AT-00554873

Speaker: Zack

GOOG-DOJ-AT-00554874

Speaker: Zack

2020 H2 Roadmap

	Reduce latency & expand enforcement	Programmatic signals, Verdicts, & leads sharing	Improve detection & classification
Summary	Align enforcement **principles and practices** across top abuse vectors	**Eliminate organizational information gaps and maximally leverage** signals and leads from across PAs	Dramatically **improve both independent and joint** ad fraud **detection & classification** recall
2020H1 Highlights	- Aligned on new Ad Fraud definition, expected to go live in July - Enforcement expanded on Google Play using the Credible Technical Evidence policy.	- SmartLeads-Marmot integration completed - Play Auto-suspend launched for high precision flags from AdSpam - Joint enforcement against Cheetah Mobile from AdSpam and Play for Disruptive Ads: $45M AAR	-Launched AdFraud2020 Dash - Landed disruptive ads dynamic detection migration from AppCrawler to Marmoset - Landed Bianca disruptive ads traffic based detection with AdMob data - Landed App CoClick Filter: $4.2M ARR - Landed Caprice filter (pTouchDuration) in ramp up: $19.7M ARR - Developed Unified PubAppRisk model: $140M ARR. - Launched Bianca disruptive ads SmartLeads generator
2020H2 Plans	- El Paso policy bundle (Oct 25) and further enforcement practice alignment. - Inactive ads policy roll out and enforcement implementation with Detox	- Magellan project: improving auto detection and using AdSpam signals to improve Marmot ability to detect - Overhaul of how ASE APK categorization are applied on ads serving	- Developing impression defences (expecting >$50M ARR) - Multisource attribution and measurement in Ad Fraud tracking - Additional SmartLeads ad fraud generators
2020EOY	**ON TRACK**	**ON TRACK**	**ON TRACK**

Google

Speaker: Zack

GOOG-DOJ-AT-00554876

Top Themes

- Disruptive ads
  - Out of context ads
    - Current out of context interstitials (outstitials)
    - Coming soon: out of context banners
  - No UI/Hidden icon apps
  - Coming soon: excessive ads
- Click fraud
  - Current: direct AdShield signal detection
  - Coming: aggregated traffic analysis (e.g. pTouchDuration pXY)
- ITC (incentivized to click)
  - AdSpam has certain level of detection
  - Need Play policy to enforce at Play store
- Impression Fraud

Google

Speaker: Xin

GOOG-DOJ-AT-00554877

DTX-951 Page 174 of 181

AdSpam, Play, Android Collaboration

- **Leadgen engine**: generate entity-level leads from our event-level detection

- **SmartLeads**: end-to-end support for leads sharing
  - leads signal compilation, sharing, result tracking, dashboard

- **Magellan**: an intelligent pipeline to run apps and detect ad fraud activities
  - Use apps traffic info to guide app automation
  - Use app automation to save leads validation cost
  - Collect ad fraud evidence efficiently

- **Bi-directional feedback loop**
  - Use AdSpam leads to help improve Play detection
  - Use Play detection feedback to improve AdSpam leadgen rules

Google

Speaker: Xin

GOOG-DOJ-AT-00554878

Challenges in Current Collaboration

- Ad fraud mechanisms become more sophisticated
    - Highly packed code
    - Cloaking
    - Blend organic and spam traffic
    - Real humans to commit ad fraud instead of pure program

- AdSpam TP, but not Play actionable
    - E.g VM-based or crowdsourcing attack

- Policy not aligned or missing
    - E.g. disruptive ads definition, no ITC policy
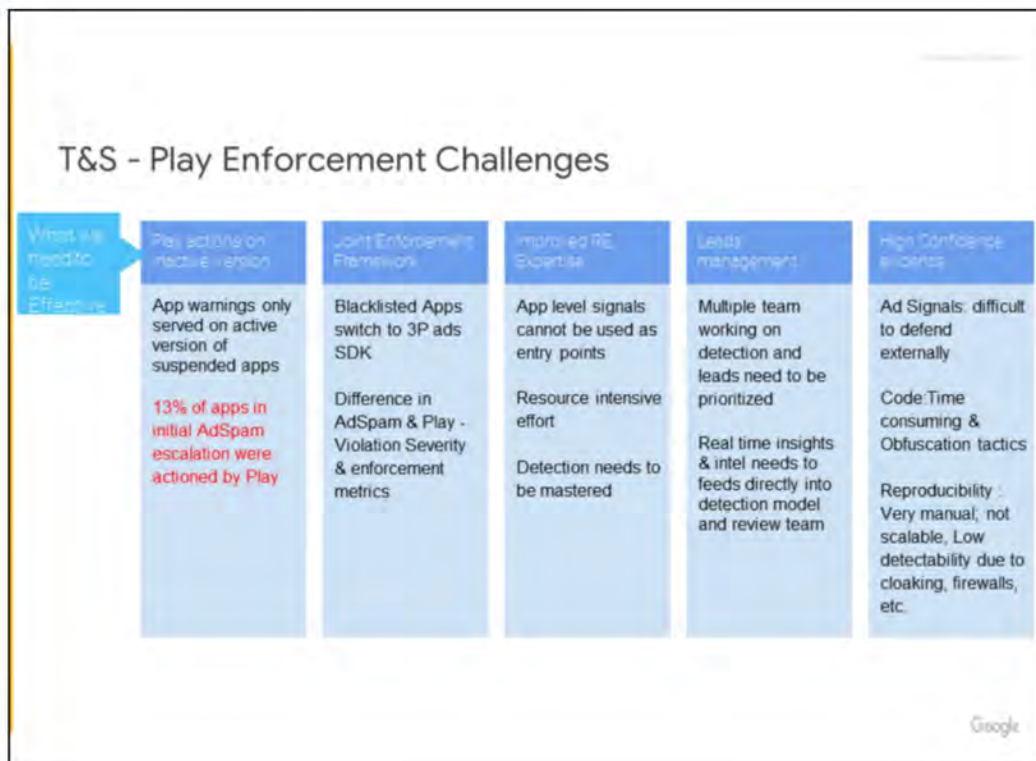
Google

Speaker: Xin

GOOG-DOJ-AT-00554879

Future Tasks

- Handling more sophisticated ad fraud
  - Highly packed code
  - Cloaking
  - Blend organic and spam traffic
  - Real humans to commit ad fraud instead of pure program
- Improve signals accuracy
  - Highly complex and diversified ad products
  - Signals not well polished
- Align and augment Play policies
  - E.g. different disruptive ads definition, no ITC policy
- Respond to threats from new areas
  - Impression fraud, webview based attack

Google

Speaker: Xin

GOOG-DOJ-AT-00554880

Speaker: Prachi

GOOG-DOJ-AT-00554881

GOOG-DOJ-AT-00554882

Reminder to provide feedback

GOOG-DOJ-AT-00554883

DTX-951 Page 180 of 181

Reminder to provide feedback

GOOG-DOJ-AT-00554884